NAVAL POSTGRADUATE SCHOOL
Monterey, California

THESIS

A TRAINING FRAMEWORK FOR THE DEPARTMENT OF DEFENSE PUBLIC KEY INFRASTRUCTURE

by

Marcia L. Ziemba

September 2001

Thesis Advisor:	Cynthia E. Irvine
Associate Advisor:	Daniel F. Warren

Approved for public release; distribution is unlimited.

Report Documentation Page

Report Date	Report Type	Dates Covered (from... to)
30 Sep 2001	N/A	-

Title and Subtitle A Training Framework for the Department of Defense Public Key Infrastructure	**Contract Number**
	Grant Number
	Program Element Number
Author(s) Marcia L. Ziemba	**Project Number**
	Task Number
	Work Unit Number
Performing Organization Name(s) and Address(es) Research Office Naval Postgraduate School Monterey Ca. 93943-5138	**Performing Organization Report Number**
Sponsoring/Monitoring Agency Name(s) and Address(es)	**Sponsor/Monitor's Acronym(s)**
	Sponsor/Monitor's Report Number(s)
Distribution/Availability Statement Approved for public release, distribution unlimited	
Supplementary Notes	
Abstract	
Subject Terms	
Report Classification unclassified	**Classification of this page** unclassified
Classification of Abstract unclassified	**Limitation of Abstract** UU
Number of Pages 114	

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** September 2001	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE: Title (Mix case letters) A Training Framework for the Department of Defense Public Key Infrastructure			**5. FUNDING NUMBERS**
6. AUTHOR(S) Marcia L. Ziemba			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A			**10. SPONSORING / MONITORING AGENCY REPORT NUMBER**
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited.			**12b. DISTRIBUTION CODE**

13. ABSTRACT ***(maximum 200 words)***

Increased use of the Internet and the growth of electronic commerce within the Department of Defense (DoD) has led to the development and implementation of the DoD Public Key Infrastructure (PKI). Any PKI can only serve its intended purpose if there is trust within the system. This thesis reviews the basics of public (or asymmetric) key cryptography and its counterpart, symmetric key cryptography. It outlines the DoD's PKI implementation plan and the user roles identified within the infrastructure. Because a PKI relies entirely on trust, training for all users of a PKI is essential. The current approach to PKI training within the DoD will not provide all of its users with the required level of understanding of the system as a whole, or of the implications and ramifications that their individual actions may have upon the system. The decentralized, segmented, and inconsistent approach to PKI training will result in a lack of trust within the PKI. Training for the DoD PKI must be consistent, current, appropriate, and available to all users at any time. The author proposes a web-based training framework for the DoD PKI. The basic requirements and design of the framework are presented, and a prototype is developed for further testing and evaluation. Without the proper attention to training, the DoD PKI will be at risk, and may not perform its intended functions of providing the required authenticity and integrity across the various networks upon which DoD conducts business.

14. SUBJECT TERMS PKI, information, training, cryptography, authentication, integrity, Internet, database			**15. NUMBER OF PAGES**
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UL

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited.

A TRAINING FRAMEWORK FOR THE DEPARTMENT OF DEFENSE PUBLIC KEY INFRASTRUCTURE

Marcia L. Ziemba
Lieutenant, United States Navy
M.G.A., University of Maryland University College, 1996
B.S., Marquette University, 1993

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN INFORMATION TECHNOLOGY MANAGEMENT

from the

NAVAL POSTGRADUATE SCHOOL
September 2001

Author: Marcia L. Ziemba
Marcia L. Ziemba

Approved by: Cynthia E. Irvine
Cynthia E. Irvine, Thesis Advisor

Daniel F. Warren
Daniel F. Warren, Associate Advisor

Dan C. Boger
Dan C. Boger, Chairman
Information Systems Academic Group

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Increased use of the Internet and the growth of electronic commerce within the Department of Defense (DoD) has led to the development and implementation of the DoD Public Key Infrastructure (PKI). Any PKI can only serve its intended purpose if there is trust within the system. This thesis reviews the basics of public (or asymmetric) key cryptography and its counterpart, symmetric key cryptography. It outlines the DoD's PKI implementation plan and the user roles identified within the infrastructure. Because a PKI relies entirely on trust, training for all users of a PKI is essential. The current approach to PKI training within the DoD will not provide all of its users with the required level of understanding of the system as a whole, or of the implications and ramifications that their individual actions may have upon the system. The decentralized, segmented, and inconsistent approach to PKI training will result in a lack of trust within the PKI. Training for the DoD PKI must be consistent, current, appropriate, and available to all users at any time. The author proposes a web-based training framework for the DoD PKI. The basic requirements and design of the framework are presented, and a prototype is developed for further testing and evaluation. Without the proper attention to training, the DoD PKI will be at risk, and may not perform its intended functions of providing the required authenticity and integrity across the various networks upon which DoD conducts business.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

I would like to acknowledge

…my husband Frank for his unconditional love, support, and understanding. He is the glue that holds our family together.

…my daughter Amber for always providing a smile when I needed it, and unending laughter at the end of a long day. Thank you sweetie.

…my father, John Haeflinger, for his rigorous encouragement of my education and my Naval career.

…my mother, Mary Haeflinger, for passing on her talents and interests in hobbies that allowed me to keep my sanity and relax during my "off" time.

…Big Frank, the proudest father-in-law a girl could ever have. I miss you.

…The other Mrs. Z, the BEST mother-in-law a girl could ever have.

…LCDR Scott Langley for his technical support and friendship (did I mention technical support?).

…LT Randy Gumke for getting me into this PKI stuff in the first place!

…Dr. Cynthia Irvine for her expertise and guidance.

…Professor Daniel Warren for his encouragement and support.

…the United States Navy for giving me this wonderful opportunity and the promise of many more adventures.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

The Internet brings information to one's fingertips and closes the distance of geographical separation. As the use of the Internet has grown in the personal and commercial sectors, it has also grown within the Department of Defense. Electronic commerce and business to business transactions have become more commonplace and have highlighted the need for additional security measures when operating over the Internet. The security measures required vary from user to user, but the Department of Defense (DoD) realized the need for a way of verifying both the identity of Internet operators as well as the information being sent across the network. In an attempt to meet this need, the implementation of a DoD Public Key Infrastructure (PKI) was planned. This thesis explains the basics of a Public Key Infrastructure, how it differs from conventional or symmetric key cryptography, and how the DoD is implementing and will continue to implement the use of a PKI within its ranks.

Problems with PKI resemble those faced when making any organizational change that involves modifying the work patterns and behaviors of employees. Additionally, the implementation of a PKI, by its very nature, is a difficult technical challenge. The strict trust requirements of a PKI together with the current inventory of DoD personnel makes the effective implementation of a DoD PKI a very challenging task. A key factor in the success of this implementation is the ability to provide the appropriate level of training to the appropriate personnel at the appropriate time. This is a challenge that, in this author's opinion, is currently on a crash course with failure. The current approach to providing user training at all levels will fall far short of the coordinated, consistent effort needed to provoke the desired result. What is the desired result? A DoD PKI with users who fully understand the implications and ramifications of their actions upon the system, and are properly trained to know what they need to do to ensure the ongoing trust of the system. With millions of users involved, this is a grand task indeed. The human element of any security system is most often its weakest link. Regarding its PKI, the DoD should be taking all the steps it can to ensure that it strengthens this weakest link as much as possible. No system is perfect, and even educated users will make mistakes, but to not attack the issue of user training aggressively is a precursor to failure.

A. PROBLEM STATEMENT

The current, segmented approach to PKI training within the Department of Defense will not provide the users with the required level of understanding and knowledge to effectively and safely use the DoD PKI. Because a PKI, by its very nature, relies on the element of trust, proper training of all users of the PKI is a key factor to the success of the PKI. Even with adequate training, users, most often the weakest link in any security chain, must be expected to make mistakes. Human beings are not perfect. The challenge comes in ensuring that the users recognize the implications and ramifications of their actions on the system as a whole and have been properly trained in how to handle circumstances in which errors were made.

B. RELATED WORK

This thesis deals with PKI, training requirements, and the development of a web-based training framework. Each of these areas has been researched and written about individually.

The PKI, although a fairly new technology, has a growing list of resources including books by Austin, and Adams and Lloyd. Austin (2001) stresses the need for fortification of information technology and reminds us that the whole system is only as strong as its weakest link. He also identifies the need to have resources underlying policies to support enforcement and provide education to users. Adams and Lloyd (1999) acknowledge the lack of experienced personnel in the area of PKI. They state that, although this deficit appears to be shrinking, organizations must recognize the need for more than a couple of administrators to run a successful PKI. They also believe that, "…it may be beneficial to institute internal training programs…to help educate the appropriate personnel" (p. 269). These authors clearly indicate the requirement for training when implementing a PKI.

On the topic of training, Hall (1998) presents a 'manual' on training management systems. He discusses what these systems are, the different types of systems available, and what these systems do. He presents numerous examples of how the different systems are being used and provides a detailed review of several existing training management systems. His point of having a consolidated system that can manage not only the training

itself, but the completion of training by individuals, is consistent with the DOD PKI training framework proposed in this thesis.

Berge (2001) focuses on the task of integrating distance training and education into a company. He addresses the current role distance training plays in business today and provides a model for organizations to use for successful incorporation of this type of learning. One area in which Berge (2001) identifies the use of distance training is to assist organizations in meeting the challenges of uncommon change (i.e. mergers or mandates beyond the direct control of the organization). This is precisely the situation that the users of the DOD PKI find themselves in.

Gery (1987) addresses the topic of computer-based training. This earlier work takes on the issues involved with computer-based training including interactivity, sponsorship, management, strategy, technology, development, standards, roles, and evaluation. Many of the obstacles of computer-based training carry over to web-based training. Although technology has advanced since the writing of Gery's book, many of the difficulties she discussed remain.

A variety of research has been done specifically on the development of web-based training. Driscoll, Alden, and Steed all provide techniques on evaluating the applicability of web-based training in a particular situation, list effective and ineffective attributes of web-based training sites, and detail a process for developing a web-based training site. The work of these authors is utilized in chapter five of this thesis.

C. A TRAINING FRAMEWORK

This thesis will focus on the training of potential and existing users of the DoD PKI. It will discuss the current training efforts and why they are not adequate to support the level of trust required even within the lowest levels of trust defined in the DoD PKI. The author will present an argument for web-based PKI training and will develop an overall framework within which this training could be provided to all who need it via existing DoD networks, hardware, and software. The product of this thesis will be a prototype of this PKI training framework that will demonstrate the basic functionality required of such a system. The goal is to provide a foundation on which an actual PKI

training system can be built. This will allow for the most efficient distribution of the most current training to widely dispersed users.

D. CHAPTER OUTLINE

This thesis contains six chapters and two appendices as follows.

Chapter I: Introduction – This chapter introduces the topic of the DoD PKI and identifies the need for appropriate training of the system's users.

Chapter II: Public Key Cryptography and Public Key Infrastructure – This chapter provides a basic overview of both symmetric and asymmetric (public key) cryptography and some implications of their use.

Chapter III: Department of Defense Public Key Infrastructure Implementation – This chapter outlines the organization of and the implementation plans for a PKI within the DoD.

Chapter IV: User Role Descriptions and Responsibilities – This chapter presents outlines the common users roles within any PKI and specifies the roles identified within the DoD PKI.

Chapter V: Training for the DoD PKI – This chapter identifies the need for training, presents the current training efforts, and introduces the idea for a web-based PKI training framework.

Chapter VI: Conclusion – This chapter summarizes the main ideas of the previous chapters and lists areas for continued research and work on this topic.

Appendix A: Database Design and Modeling – This is a basic overview of the database design and modeling techniques used in the development of the DoD PKI training database.

Appendix B: DoD PKI Training Framework Prototype – This is a compilation of screen shots from the DoD PKI Training Framework prototype.

II. PUBLIC KEY CRYPTOGRAPHY AND PUBLIC KEY INFRASTRUCTURE

Cryptography is an integral part of a Public Key Infrastructure (PKI). This chapter presents a general overview of cryptography, what it is, what communication protection services it provides, and the two types of cryptography that can be utilized. An introduction to PKI and its components follows.

A. CRYPTOGRAPHY

Cryptography involves the study of mathematical techniques and their application to certain aspects of information technology (Menezes, van Oorschot, and Vanstone, 1996). Cryptography is about preventing and detecting cheating or other malicious activities that may occur within an information system (Menezes et al, 1996). Cryptosystems provide four main services for communications protection – secrecy (or confidentiality), authenticity, integrity, and non-repudiation. Secrecy (or confidentiality), the original purpose of cryptosystems, requires that intruders are not able to determine the plain text message corresponding to a given cipher text, and that key reconstruction cannot be performed by examining cipher text for known plain text. Authenticity allows a receiver to verify the source of a message. Integrity allows a user to ensure that a message has not been modified accidentally or deliberately during transmission. Non-repudiation prevents a sender from later denying transmission of a message. Cryptosystems utilize keys to encrypt (encode) and decrypt (decode) messages. Two two types of cryptosystems can be used: symmetric key or public key (Austin, 2001). Austin provides the following summary of these essential services:

- Confidentiality *assures you* that your information is protected.
- Authentication *assures you* that you know with whom you're doing business.
- Integrity *assures you* that information is not being modified or substituted.
- Non-repudiation *assures you* that the originator cannot deny originating a message or business transaction. (Austin, 2001, p. xv)

B. CONVENTIONAL (SYMMETRIC) KEY CRYPTOGRAPHY

In symmetric key cryptography, a message is encrypted and decrypted with the same key. See Figure 2.1.

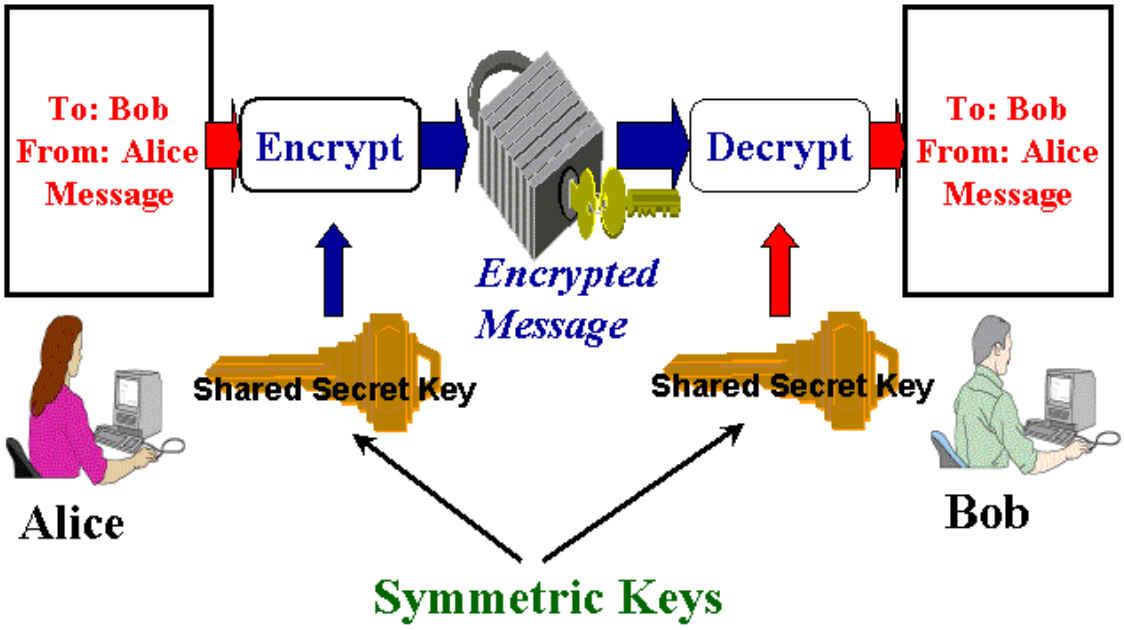

Figure 2.1 Symmetric Cryptography (From Morris, 2001, p. 5)

This requires that both the sender and the receiver possess the same key. Symmetric key encryption requires that the parties involved keep the key secret. If the key is compromised, it can no longer be used. Because this type of encryption requires that keys be distributed securely, it has several limitations (Adams and Lloyd, 1999). Key distribution and key management becomes much more difficult as the population of users grows, it is difficult to initiate communications between unknown parties, and confidentiality between specific parties requires separate keys (Morris, 2001). A mechanism for updating keys must also be in place, as the same key cannot be used indefinitely.

C. PUBLIC (ASYMMETRIC) KEY CRYPTOGRAPHY

Public key cryptography provides the same services as symmetric key cryptography in general, but it uses different keys for encryption and decryption. A key pair in a public key cryptography scheme consists of a private key and a public key. These key pairs are generated by a process that ensures the keys are uniquely paired with one another and that neither key can be determined from the other (Hale and Friedrichs, 2000).

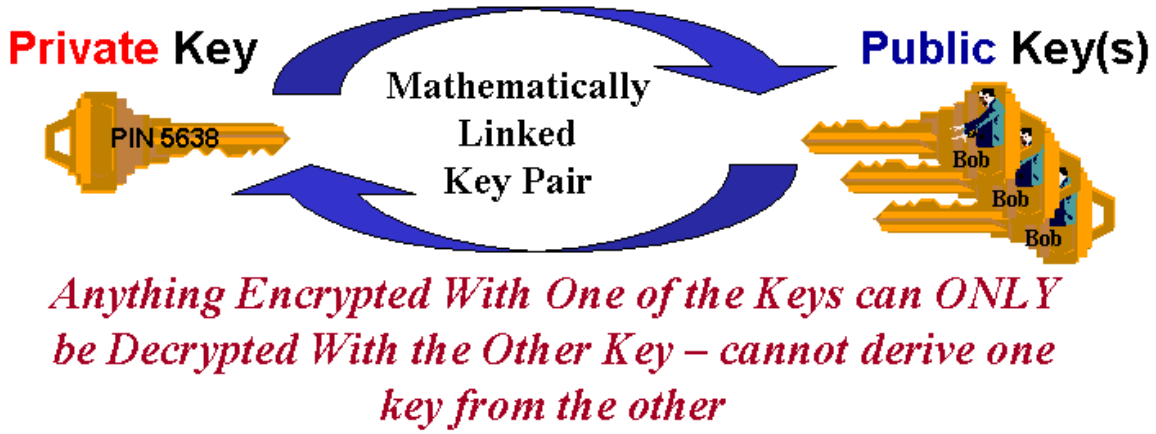

Figure 2.2 Asymmetric Encryption (From Morris, 2001, p. 7)

Each entity in a public key system will be assigned a private key and a public key. Private keys are kept private, and public keys are published and accessible to anyone (www.iplanet.com, 2000). The process of sending a message using a public key system is as follows:

- Alice wants to send a message to Bob so that Bob is the only one who can read the message (confidentiality).
- Alice has Bob's public key.
- Alice encrypts the message with Bob's public key.
- Alice sends the encrypted message to Bob.
- Bob uses his private key to decrypt the message.

In this scheme, Bob, who is in sole possession of Bob's private key, is the only one who will be able to decrypt this message. If the message is intercepted during transmission, the interceptor will not be able to decrypt it. This process is described in general in Figure 2.3.

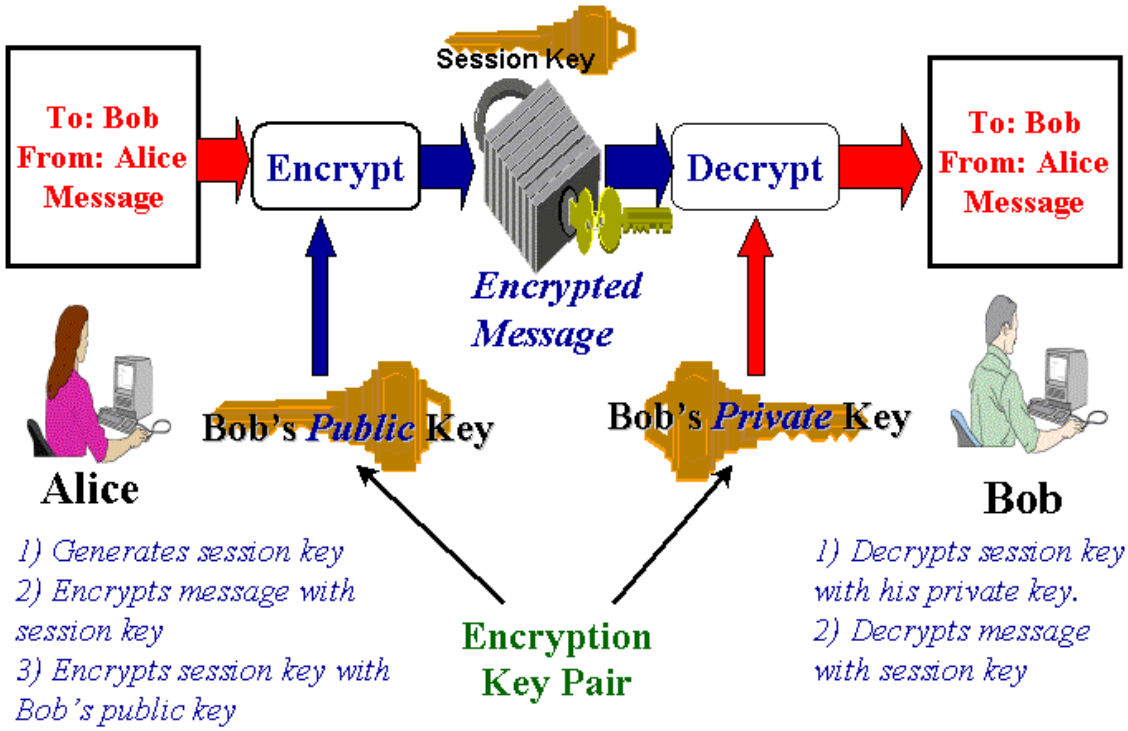

Figure 2.3 Asymmetric Encryption (Confidentiality) (From Morris, 2001, p. 8)

The reverse of this scenario is also utilized for signing messages with a digital signature. A digital signature is an electronic document that describes the holder (www.id2tech.com, 2000). The recipient of a digitally signed message, having the public key of the signer, can determine 1) if the message was created with the signer's private key, and 2) if the message has been altered since it was signed (ASD Memo, 2000). Digital signatures provide authentication, non-repudiation, and integrity checks. In a public key system, encrypting a message with a private key is effectively signing the message since only one person has the private key (Austin, 2001). When using a digital signature, the data itself is not encrypted, but a hash of the data is encrypted with a private key. A hash is a number of fixed length such that 1) the value of the hash is unique for the hashed data and any change in the data results in a different value, and 2) the content of the hashed data cannot be deduced from the hash itself (resulting in the use of the term "one-way hash"). Figure 2.4 illustrates the use of a digital signature.

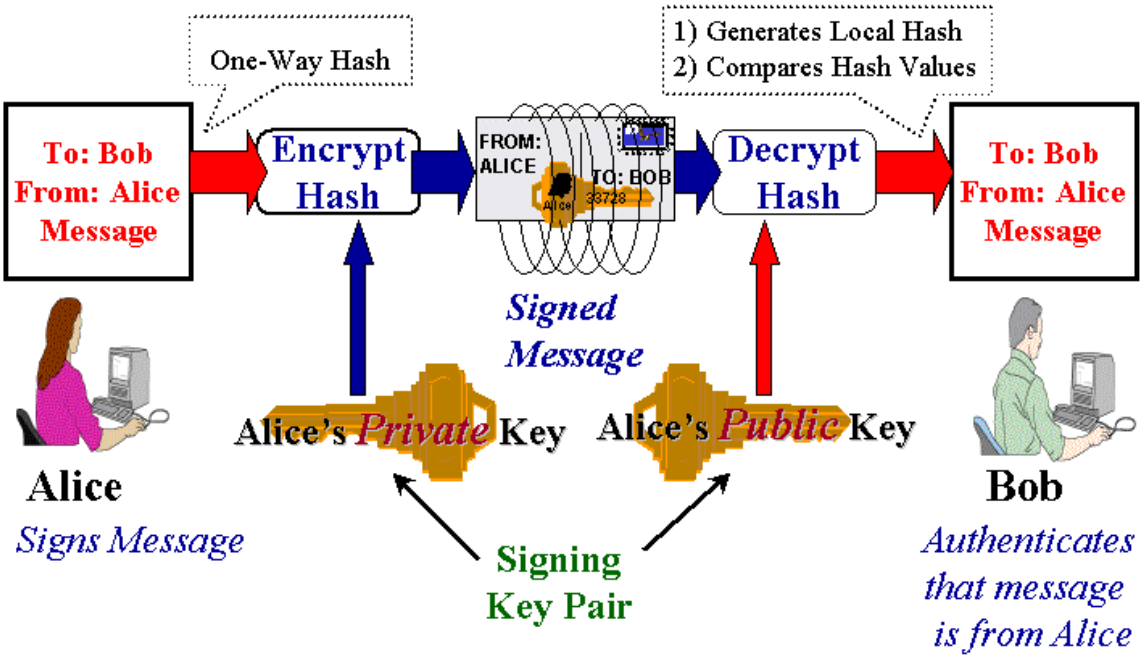

Figure 2.4 Digital Signing (Authentication, Integrity, Non-repudiation) (From Morris, 2001, p. 9)

In Figure 2.4, the data and the digital signature are sent to the recipient. The digital signature is simply a one-way hash of the original data that has been encrypted with the signer's private key. To validate the data, the recipient uses the signer's public key to decrypt the digital signature and obtain the hash. The original data is then run through the same hashing algorithm that generated the original hash. Information about the hashing algorithm is actually included with the digital signature (although it is not shown in the figure). This new hash is compared to the original hash to verify that the data has not been changed since it was signed. (www.iplanet.com, 2000)

Public key encryption and digital signatures are often combined to provide all four services (confidentiality, authentication, integrity, and non-repudiation). In this situation, a message is signed with the sender's private key and the recipient's public key. This ensures that only the intended recipient will be able to read the message, and that the data has not been compromised and actually came from the stated sender.

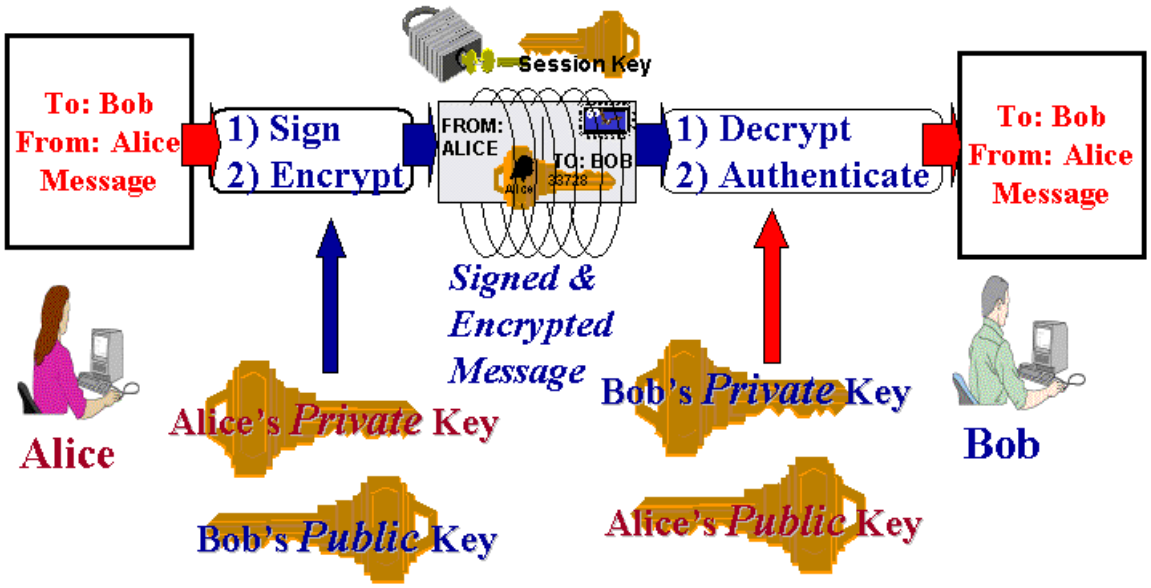

Figure 2.5 Digital Signing and Encrypting (From Morris, 2001, p. 10)

This seems, on the surface, to be a valid method of ensuring integrity of data and authenticating the sender. However; how can the receiver be certain that a digital signature is valid? An imposter could substitute his or her public key for someone else's, and the receiving party would not be able to tell the difference. In order for public key encryption to be valid, a level of trust must exist within the system. This trust is established through the use of certificates and Certification Authorities within a public key infrastructure.

D. PUBLIC KEY INFRASTURCTURE COMPONENTS

1. What is a Public Key Infrastructure?

A Public Key Infrastructure has many definitions. The following list provides a sample of some of these definitions.

From Morris (2001, p. 15), a PKI is "…personnel, policy, procedures, components and facilities to enable public key cryptographic functions so that applications can provide the desired security services."

From Green (2001, p. 3), a PKI is "personnel, policy, procedures, components and facilities to bind user names to electronic keys so that applications can provide the desired security services."

From DoD Class 3 PKI CONOPS (1999, p. 2-5), a PKI is "…that portion of the security management infrastructure dedicated to the management of keys and certificates used by public key-based security services."

Essentially, a PKI includes all the components required to establish and maintain the trust relationship and the binding of a public key to its owner within a system providing public key-based applications. "Most important is the fact that with IT security, just as with military security or castle fortification, security is only as good as its weakest components." (Austin, 2001, pp. 23-24)

2. Primary PKI Elements

A Public Key Infrastructure is comprised of 3 basic elements or processes. These are 1) certificate management, 2) the registration process, and 3) public key-enabled applications. Within these elements are various components. These components can be broken down into people, hardware, and policies. (Morris, 2001)

The people component can be broken down into various roles. These roles include the Certification Authority (CA) – who creates and signs public key certificates, the Registration Authority (RA) – who authorizes the creation of a certificate and provides information to the CA, the Subscriber (or end user) – who requests certificates and uses keys in applications, and the Relying Parties – the applications and users who trust the certificates. (Morris, 2001)

The hardware components of a PKI include the Repository (or Directory) – the device used to store and retrieve public key certificates, keys, and revocation information (Morris, 2001), workstations, firewalls, routers, and servers (Galik, 2000). Workstations, firewalls, routers, and servers are examples of non-human entities that may be subscribers to a PKI (Galik, 2000). The specific guidelines regarding these types of subscribers are described in the PKI policies.

Policies are those documents which define the rules and processes of the PKI system (Galik, 2000). Within these policy documents are the levels of assurance that will be required (Galik, 2000). The assurance levels defined for the DoD PKI are defined in Chapter III.

E. CERTIFICATES AND CERTIFICATION AUTHORITIES

Certificates and Certification Authorities are used in a public key encryption system to build confidence into the system. A Certification Authority (CA) verifies the authenticity of a public key. CAs produce identity certificates that include an individual's public key. For example, an identity certificate for Alice would include Alice's name, the name of the CA that issued the certificate, Alice's public key, a period of validity, a serial number, and additional technical parameters (www.iplanet.com, 2000). The trusted CA then signs the certificate with its private key. Now the certificate can be published and used by other individuals doing business with Alice with the confidence of knowing that the CA has verified that the public key truly belongs to Alice (Hale, 1999). In effect, the identity certificate binds Alice's identity to her public key, but how does the CA know that it is really Alice's public key being signed? In order to obtain the necessary information to create Alice's certificate, another trusted entity called the Registration Authority (RA) is involved. The RA is an intermediary between Alice and the CA. The RA is responsible for identifying Alice and authorizing her to get a certificate. Working together, Alice, the RA, and the CA verify Alice's identity and public key, issue Alice's identity certificate, and ensure that Alice, and only Alice, possesses the matching private key. (Hale, 1999)

Several certificate formats exist, but the most widely accepted format is that of the X.509 standard. The International Telecommunication Union (ITU-T) developed the X.509 standard in 1988. A second version of the standard was released in 1993, and it included additional fields. The structure of version two was determined to be too restrictive, and it was replaced by version three in 1996. (java.sun.com, 1998) Refer to Tables 2.1 and 2.2 for details on the X.509 v3 certificate standard.

<table>
<tr><td colspan="3">Version (of Certificate Format)</td></tr>
<tr><td colspan="3">Certificate Serial Number</td></tr>
<tr><td colspan="3">Signature Algorithm Identifier (for CA’s Signature)</td></tr>
<tr><td colspan="3">Issuer (Certification Authority) X.500 Name</td></tr>
<tr><td colspan="3">Validity Period (Start and Expiration Date/Times)</td></tr>
<tr><td colspan="3">Subject Name (X.500 Name)</td></tr>
<tr><td colspan="3">Subject Public Key Information
Algorithm Identifier
Public Key Value</td></tr>
<tr><td colspan="3">Issuer Unique Identifier</td></tr>
<tr><td colspan="3">Subject Unique Identifier</td></tr>
<tr><td colspan="3"></td></tr>
<tr><td>Extension Type</td><td>Critical/Non-critical</td><td>Extension Field Value</td></tr>
<tr><td colspan="3">Certification Authority’s Digital Signature</td></tr>
</table>

Table 2.1 X.509 v3 Certificate Format (After Gaines, p. 83)

Element	Description
Version	This lists the version of the certificate that is being used. In most cases this will be version 3.
Serial number	An integer value assigned by the CA that uniquely identifies the certificate.
Signature algorithm identifier	This field identifies the algorithm used to digitally sign the certificate and any related parameters.
Issuer name	X.500 name of the CA that created and signed the certificate.
Validity period	This field lists the start and expiration dates of the certificate.
Subject name	This is the name of the entity that corresponds to the public key. Previous versions only allowed X.500 names, but version 3 allows additional naming formats.
Subject public key information	This field lists the algorithm, parameters and public key of the entity in the subject name field.
Issuer unique identifier	This is an optional field that contains additional information about the CA.
Subject unique identifier	This field is optional and contains additional information about the subject to ensure name collisions do not occur.
Extensions	This field is optional. X.509 v3 supports numerous extension fields depending on the applications' need.
Issuer's signature	This field contains the algorithm identifier, parameters and the certificate hash signed by the CA's private key.

Table 2.2 X.509 v3 Certificate Elements (After Gaines, p. 83-84)

In addition to the Identity Certificate, which provides for authentication, non-repudiation, and integrity, there are several other certificate types. All certificate types are described briefly in the following table.

Certificate Type	Services Provided
Identity	Authentication, non-repudiation, integrity
Email Signing (encryption)	Authentication, non-repudiation, integrity
Server/Device	Web server authentication, encryption via SSL

Table 2.3 Certificate Types (After Morris, 2001, p. 24)

F. PROTECTION OF PRIVATE KEYS

CAs provide verification of an individual's public key, but the other half of public key encryption, the private key, introduces additional problems into a public key system. The protection of private keys is essential in a public key encryption system. A private key is tied to one individual, and, if this tie is broken, the public/private key pair issued becomes invalid. Two options for storing private keys are: software encryption or the use of a token. Software encryption will protect a private key as long as the password to access the key is not compromised. This type of protection may be appropriate when a computer has a single user and has some level of physical isolation from others (i.e. – an office door with a lock). A token is a device that is used for protection and transportation of private keys of a user. These can be floppy disks, smart cards, common access cards, PC cards, or others (ASD Memo, 2000). Tokens allow more flexibility in that the private key is not simply stored on one computer, but it is mobile and does not rely on the use of the same computer all the time. These may be appropriate when multiple users share the same computer or when individuals have a need to travel and use their private keys in a variety of locations. Hale and Friedrichs (2000) note that there is currently widespread storage of private keys in an encrypted file accessed only via password, but that there will be a move, within the Department of Defense, toward some type of hardware token. It is expected that the Common Access Card (CAC) will become the primary token for class 3 and 4 PKI certification levels (ASD Memo, 2000). If a private key is lost or compromised, the PKI must support the notification of its users that a particular key pair is no longer valid and should not be used or trusted. This notification is conducted via the use of Certificate Revocation Lists (CRLs). CRLs are discussed in more detail in the following section. All of the user roles within a PKI system must act promptly as soon as

a private key is lost or compromised so that the system can remain as up to date and trustworthy as possible. Proper training must be provided to ensure that all users have an understanding of what to do and when to do it.

G. CERTIFICATE REVOCATION LISTS

A public/private key pair becomes unusable if the private key is lost or compromised. When this occurs, there must be procedures in place to notify all potential users of the public key encryption system that the public key is no longer valid. This is normally done through a Certificate Revocation List (CRL). A CRL is generated, signed, and published by a CA. The process normally occurs as follows:

- Alice is issued a public/private key pair.
- A CA creates, signs, and publishes a certificate containing Alice's public key.
- Alice loses her private key and notifies the RA that initially authorized her to obtain the certificate. If the RA is not available, Alice may contact the CA directly to report the loss of her private key.
- The RA notifies the CA that issued Alice's certificate that her private key has been lost.
- The CA adds Alice's certificate to its CRL, which is signed and published at frequent intervals.

Ensuring that the information in a PKI directory is current and trustworthy is crucial to the trustworthiness of the PKI system as a whole. The procedures in place within the system and the practices followed by users at all levels will determine the degree to which the system can and should be trusted.

Loss or compromise of a private key is not the only reason that a certificate may have to be revoked. A certificate will be revoked if any of the information it contains is no longer valid. Because of this, it is important that a certificate contain only information that is unlikely to change frequently. Any compromise in the certificate issuing or maintenance process will also necessitate the revocation of a certificate (Hale, 1999).

H. KEY ESCROW, KEY RECOVERY, AND DATA RECOVERY

Key escrow, key recovery, and data recovery are used to support obtaining access to information protected by a public key system in which the originator of the data is unable or unwilling to provide access. Key escrow involves copying and storing confidentiality (or encryption) private keys for use in predefined situations. When one of these situations occurs, the private key can be recovered and used to access any information that was encrypted with the key. Situations in which data and key recovery may be required include an employee forgetting the password required to unlock an encrypted file, the loss of a hardware token containing the key required to unlock an encrypted file, or the death of an employee who had stored encrypted information. Key escrow and recovery must exist in order for data recovery to occur. Systems for key escrow and recovery must provide a secure method of storing the copy of a user's private encryption key. Authorized key recovery agents are allowed to retrieve a copy of a user's key under certain conditions. Once the key is recovered, the encrypted data can be accessed. Key and data recovery are used for encryption keys only. User's private signature keys are not recoverable. (DoD Class 3 PKI CONOPS, 1999) (SPAWAR, 2000)

I. VULNERABILITIES AND CHALLENGES OF PUBLIC KEY CRYPTOGRAPHY AND THE PUBLIC KEY INFRASTRUCTURE

The success of public key cryptography relies on many factors. A successful and trustworthy PKI, at a minimum, relies on the process of issuing certificates, the protection of individual private keys, the protection of the CA's private key, and the accuracy and timeliness of CRLs. Because the system is a chain, if any one of these links fail, the system fails. It is vital to a PKI system that all of these links, including human links, be reinforced, to the highest degree possible, to maintain the level of security required. The integrity of this chain is one of many challenges that come with implementing a public key infrastructure. Other challenges include training, ease of use, interoperability, scalability, and key escrow processes (Morris, 2001) (Galik, 2000). Some safeguards that can be put in place in a PKI system are policies to ensure consistent procedures for issuing certificates, checks and balances to provide internal and external reviews and audits, and, arguably the most important safeguard, a comprehensive, role-specific,

timely training program (Hale, 1999). For the Department of Defense, the critical factors for a successful PKI implementation will include flexibility, coordination, and training (Morris, 2001).

Chapter III will delineate the Department of Defense plans for implementing a PKI. The DoD PKI will be one part of the overlapping layers of protection of the overall Defense in Depth strategy. The planned DoD PKI organization, assurance levels, services, and architecture will be discussed.

III. DEPARTMENT OF DEFENSE PUBLIC KEY INFRASTRUCTURE IMPLEMENTATION

The Department of Defense has recognized the need for a PKI, and it has laid out plans for its implementation. This chapter provides an overview of how a PKI fits into the overall DoD information assurance posture and the DoD PKI implementation strategy as a whole.

A. DEPARTMENT OF DEFENSE INFORMATION ASSURANCE

The Department of Defense utilizes an Information Assurance policy called Defense in Depth. This policy requires the implementation of multiple layers of overlapping protection for information systems. This overlapping system of defense is designed to protect DoD assets and assure successful mission execution. A graphical representation of this Defense in Depth strategy is contained in Figure 3.1 below.

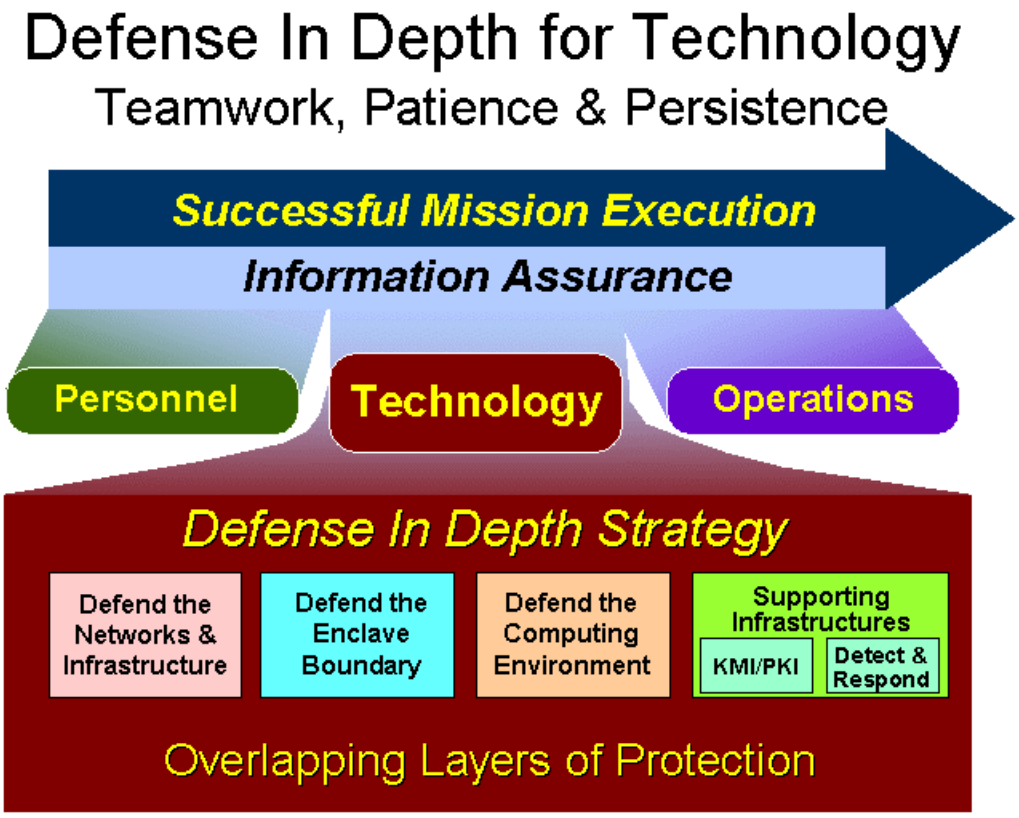

Figure 3.1 Department of Defense – Defense in Depth (From Green, 2001, p. 26)

The Defense in Depth strategy relies on the use of a

> …common, integrated, interoperable DoD PKI to enable security services at multiple levels of assurance. The goal of this DoD-wide infrastructure is to provide general-purpose PKI services to a broad range of applications, at levels of assurance, consistent with operational imperatives. (ASD Memo, 2000, p. 2)
>
> The implementation of PKI technology within the DoD is a large, complex and challenging task and is essential for achieving our defense in depth goals. (Galik, 2000, p. 6)

B. DOD PUBLIC KEY INFRASTRUCTURE ORGANIZATION

On August 12, 2000, the DoD Chief Information Officer (CIO) issued a memorandum issuing and updating policies regarding the development and implementation of a DoD PKI (ASD Memo, 2000). The National Security Agency (NSA) has been assigned as the Program Manager for the DoD PKI effort with a Deputy Program Manager provided by the Defense Information Systems Agency (DISA) (Galik, 2000). The following chart shows the organization of the DoD PKI Program Management Office as of January 2001:

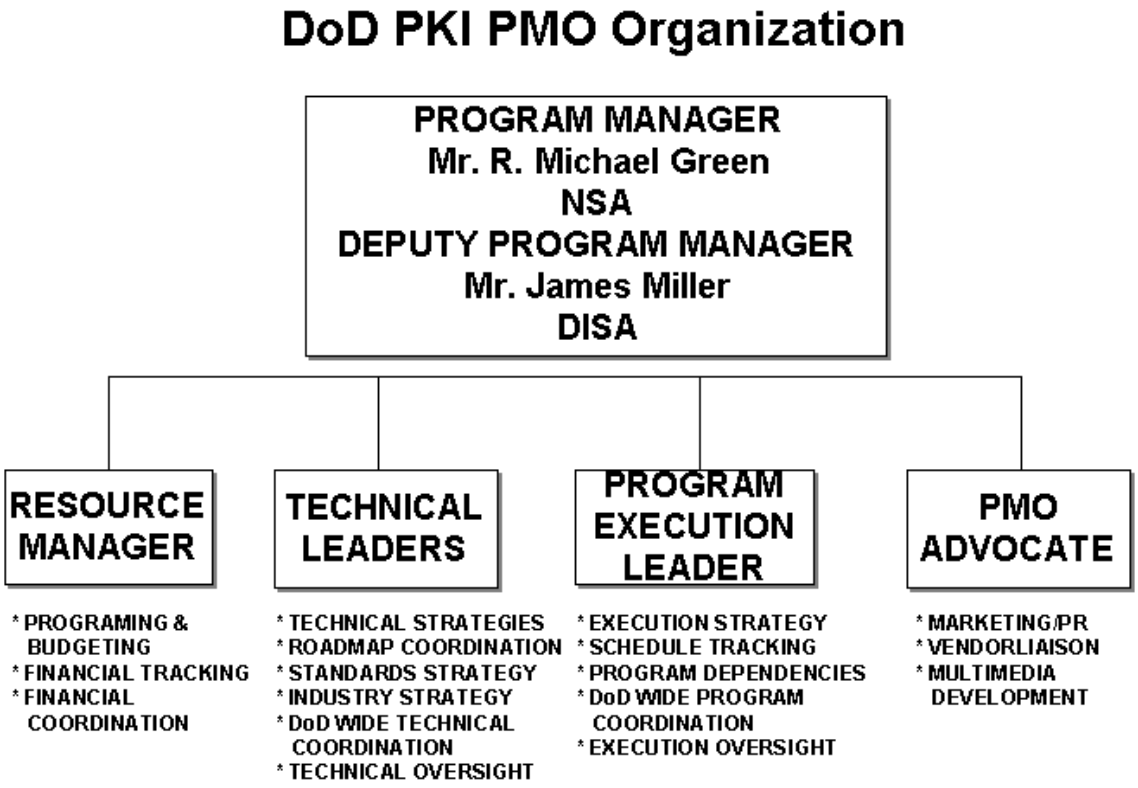

Figure 3.2 DoD PKI PMO Organization (From Green, 2001, p. 12)

The DoD CIO's memorandum also included a delineation of responsibilities for certain key individuals and offices regarding the implementation of the DoD PKI. The DoD CIO is responsible for management of the Defense-wide Information Assurance Program (DIAP) which includes providing oversight of DoD PKI activities, developing PKI planning guidance, providing guidance on PKI implementation and integration, and study technical issues regarding PKI-enabled access to classified DoD networks and classified private web servers. (ASD Memo, 2000)

The DoD Components (The Office of the Secretary of Defense, the Military Departments, the Chairman of the Joint Chiefs of Staff, the Combatant Commands, the Inspector General of the Department of Defense, the Defense Agencies and Offices, and the DoD field activities) are responsible for

> …planning, programming, and budgeting to implement the DoD PKI according to this policy and to develop the required policy and plans to ensure a standard implementation of the DoD PKI within their respective organizations…" (ASD Memo, 2000, p. 5)

These high-level responsibilities filter down ultimately to the CAs, RAs, LRAs, and users of the DoD PKI. The identification of the various roles within the DoD PKI and their responsibilities is contained in Chapter IV.

C. PKI CERTIFICATION/ASSURANCE LEVELS

A PKI assurance level is the degree of confidence one can place in the binding the PKI creates between a person and his or her private key (Hale and Friedrichs, 2000). The Department of Defense has defined four different levels of assurance regarding PKI and explained the circumstances under which three of these levels will be implemented. These levels are defined in Appendix C of the Public Key Infrastructure Roadmap for the Department of Defense (DoD PKI PMO, 1999).

1. Class 3: (Formerly Medium)

> This level is intended for applications handling medium value information in a low to medium risk environment. This assurance level is appropriate for applications that require identification of an entity as a legal person, rather than merely a member of an organization. This assurance level requires that the end user register in person and their cryptography can be software based. (DoD PKI PMO, 1999, p. C-1)

2. Class 4: (Formerly High)

> This level is intended for applications handling medium to high value information in any environment. These applications typically require identification of an entity as a legal person rather than merely a member of an organization and a cryptographic hardware token for protection of the private key material. This level requires a hardware token for protection of private key material, and that the end user register in person. (DoD PKI PMO, 1999, p. C-1)

3. Class 5

> This level is intended for applications handling high value information in a high-risk environment. This assurance level requires National Security Agency (NSA)-approved Type I cryptography. (DoD PKI PMO, 1999, p. C-2)

D. DOD PKI SERVICES

In order to support the security services required by a PKI, the DoD PKI will provide the following services (DoD PKI CONOPS, 1999):

1. Key Generation

This is the process of generating the key pairs – one public and one private that will enable public key functionality.

2. Certificate Generation

This is the process of issuing a certificate after a key pair has been generated. This process may be combined with the key generation process, or it may be requested by users who generate their own key pairs. When requested by a user, a registration process must be completed in which the user provides the required information to a CA, and the CA creates a certificate and signs it with the CA's private key. The requirements for this registration process are established in the CA's Certification Practice Statement. These requirements are essential to the PKI system because it is this certificate that will provide the trusted binding between a key pair and its owner.

3. Certificate Revocation

Certificate revocation is required when a certificate becomes invalid, for any of several reasons, prior to its expiration date. Some of these reasons include compromise of the private key (through loss or deception), or when any of the information contained in the certificate is no longer valid. It is for this reason that the information used in the certificate should be of the type that does not change frequently. This will lessen the need to revoke and reissue certificates more frequently than absolutely necessary to protect the integrity of the PKI.

4. Certificate Expiration, Update, and Rekeying

Certificate expiration is a built-in mechanism for limiting the life of a certificate. This limit is imposed to help protect the key against compromise and ensure that the information in the certificate remains current. Owners of certificates must obtain new certificates prior to the expiration of their current certificates in order to avoid a disruption in service. This can be accomplished through updating or rekeying a certificate. This process is very similar to the process of generating a key pair for the first

time except that the owner utilizes his or her current key pair to authenticate themselves to the CA during the registration process. The registration process is repeated to ensure that the owner's need for the certificate still exists.

5. Archiving

Archives must be maintained so that signatures on old documents may be verified even after the CA that issued the certificate used to sign the document is gone. These long-term repositories must archive certificates that have been issued, certificate revocation lists, and user registration information.

E. DOD PKI CA ARCHITECTURE

The goal for the DoD PKI architecture is to employ centralized certificate management with decentralized registration. Figure 3.3 displays the target DoD PKI CA architecture (DoD PKI PMO, 1999, p. 7).

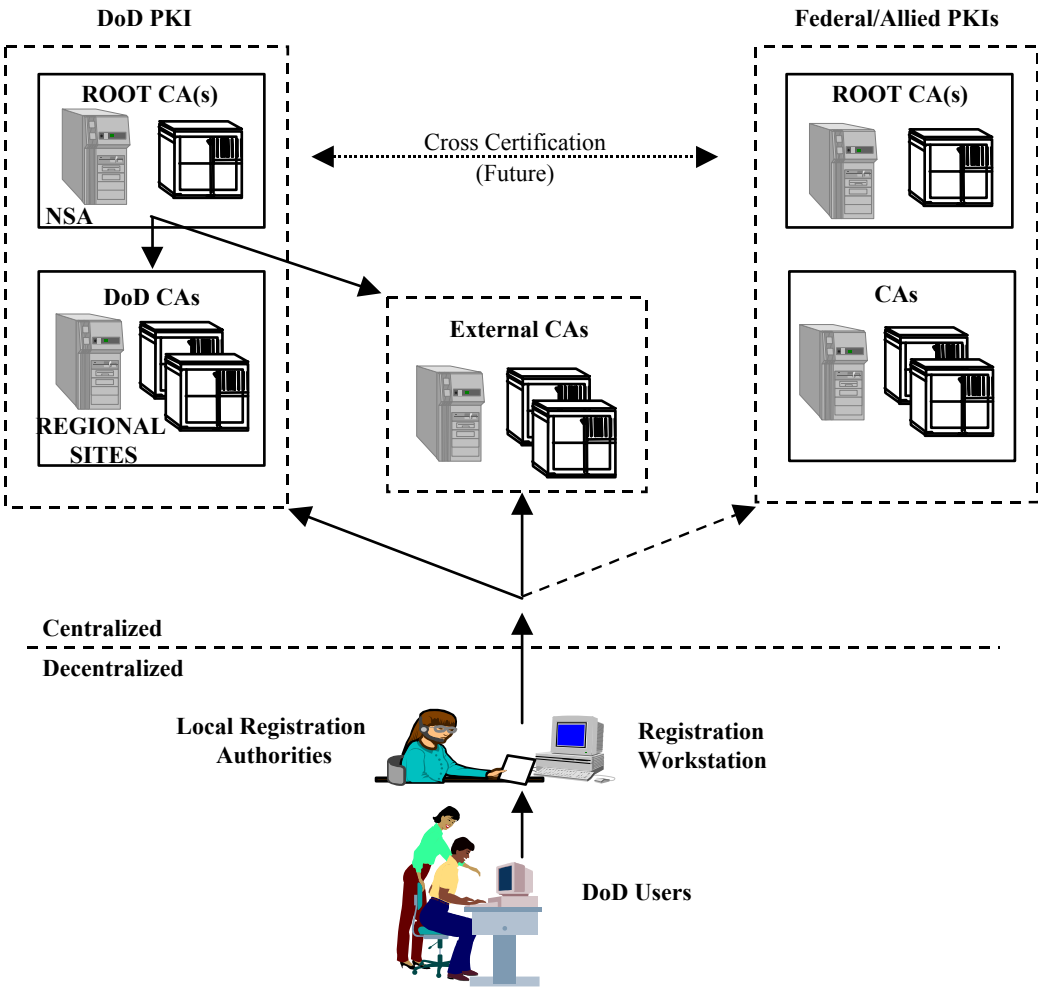

Figure 3.3 Target DoD PKI CA Architecture (From DoD PKI PMO, 1999, p. 7)

The main levels of this architecture, as shown in Figure 3.3, are the centralized Root CA and DoD CAs, and the decentralized RAs, LRAs, and DoD Users. These specific roles are described in detail in Chapter IV. Additional entities of the DoD PKI include a Data Recovery Manager (DRM), CRL Archive Servers, Directories, Archives, and Certificate Status Servers.(DoD Class 3 PKI CONOPS, 1999)

A Data Recovery Manager (DRM) allows for the recovery of a user's key. The circumstances in which the DRM may be used to recover a key include those circumstances listed in Chapter II under Key Escrow, Key Recovery, and Data Recovery and may also be authorized by a user's Commanding Officer under additional circumstances. These circumstances are not spelled out in detail, but it is assumed that they may include instances in which illegal activity is suspected. The DoD PKI version 2

will employ a central team of key recovery agents to perform this function. (DoD Class 3 PKI CONOPS, 1999)

A CRL Archive Server allows a user to verify a digital signature by providing long-term storage and retrieval of CRLs. This is required to obtain verification of old messages or documents that were signed using a certificate that has since expired. The verification of these certificates must be done by accessing the CRL Archive Server and checking the CRL that was in effect at the time that the signature was made. (DoD Class 3 PKI CONOPS, 1999)

Directories are those entities of a PKI that store information about users and their certificates. Directories are maintained by CA's who post certificates to the directory upon their creation. Directories are where users of a PKI gain access to the public keys and certificates of other users. Directories also store CRLs so that a determination of validity can be made regarding an inquiry on any certificate posted to the directory. (DoD Class 3 PKI CONOPS, 1999) The target DoD PKI architecture calls for a common "…DoD-wide directory to support all DoD public key enabled applications." (DoD PKI PMO, 1999, p. 9)

Archives contain the weekly backup copies of CA system configuration files (archived at initialization), certificates, CRLs, weekly audit logs, and any modifications to the CA system configuration files. These archives will be maintained for 10 years and 6 months. (DoD Class 3 PKI CONOPS, 1999)

An Online Certificate Status Server enables the real time or near real time determination of the validity of a certificate by querying a dedicated server. The protocol used for this is the Online Certificate Status Protocol. (DoD Class 3 PKI CONOPS, 1999)

F. DOD PKI STRATEGY AND MILESTONES

The Department of Defense has defined a strategy for implementing its PKI and has defined the following milestones (approved 12 August 2000):

- December 2000 – private web servers will be PKI-enabled
- December 2001 – the complete class 3 infrastructure will be in place

- October 2002 – all DoD personnel will be issued class 3 certificates
- October 2002 – all DoD e-mail must be signed with al class 3 certificate
- October 2002 – all private web servers must perform client-side authentication
- October 2002 – the issuance of class 4 certificates will begin
- December 2003 – migration of mission critical systems from class 3 to class 4 protection (Green, 2001)

G. DOD PKI TRAINING

Based on the Public Key Infrastructure Roadmap for the Department of Defense,

> CINCs, Services, and Agencies that operate PKI equipment will acquire appropriate training for their operators on the policy and proper use of the equipment. The Program Management Office, working with the Services, will develop the training material for any equipment that they develop. (DoD PKI PMO, 1999, p. 22)

Currently, DoD PKI training is handled primarily through the Information Assurance Support Environment – supported by the Defense Information Systems Agency. This web site provides general information, documents related to PKI, and a schedule of PKI training currently being offered. There is also a DoD PKI Help Desk which can be accessed via the Internet or by phone. The help desk provides assistance to all DoD PKI users 24 hours a day.

The training is not currently widely available, and the Help Desk provides only a reactive response to problems. A more comprehensive, widely available training source for DoD PKI users needs to be implemented. In order to provide the required level of trust in a PKI, all components must be equally secure. This includes the human components.

H. CONFIDENTIALITY VS. IDENTITY CERTIFICATES

Within the DoD PKI, two types of certificates will be issued and used. The identity certificate uniquely identifies a user while a confidentiality or encryption certificate encrypts data. (SPAWAR, 2000)

I. KEY ESCROW AND KEY RECOVERY

The DoD PKI will require key escrow (as explained in Chapter II) for its confidentiality or encryption certificates. This will ensure that encrypted data can be recovered in the event a person dies, loses their private encryption key, or leaves the DoD. (SPAWAR, 2000) Within the DoD PKI, only the user and the commanding officer may request recovery of an escrowed key. Key recovery is protected by two-person integrity, meaning two key recovery agents are needed to recover a key. The specific processes involved in key recovery within the DoD PKI are explained in Chapter V. (DoD Class 3 PKI CONOPS, 1999)

The implementation of a PKI within the DoD is a complex task that will involve many people and a significant amount of time and resources. The people involved in the implementation and the day-to-day operations of the PKI will serve in various roles with various levels of responsibility. It is important that these responsibilities are well defined and well understood. Chapter IV will discuss the basic human roles in a generic PKI as well as define the specific roles that will be filled within the DoD PKI.

IV. USER ROLE DESCRIPTIONS AND RESPONSIBILITIES

A PKI relies on the performance of specific tasks by specific entities within the system. Several of these roles are standard and can be found in any PKI. The DoD utilizes these standard roles and some additional roles in its PKI implementation. This chapter describes these roles and their inherent responsibilities.

A. PKI USER ROLES

All PKI systems include various types of users. These users or components of a PKI have certain responsibilities that must be fulfilled to assure that the PKI services are maintained at the desired level of security. Adams and Lloyd describe several of the key user roles involved in any PKI system and their responsibilities (Adams and Lloyd, 1999):

1. Subscriber

A subscriber is an end-user who acquires a certificate for subsequent use within the PKI system. These end-users are obligated to:

- Make truthful representations in applying for a certificate
- Review and accept a certificate before using it
- Make certain representations upon acceptance of the certificate
- Control and keep confidential the corresponding private key
- Promptly revoke the certificate upon compromise of the corresponding private key (Adams and Lloyd, 1999, p. 192-193)

Upon acceptance of a certificate, a user must verify his or her identity to the agent presenting the certificate, and agree to use the certificate as it is intended to be used.

2. Certification Authority

A Certification Authority is an independent and trusted third party that certifies the binding between and individual and his or her private key (Austin, 2001). A Certification Authority is obligated to:

- Use a trustworthy system
- Disclose its practices and procedures
- Properly identify a prospective applicant for a certificate
- Publish issued certificates in a repository
- Suspend and/or revoke certificates
- Make warranties to the certificate applicant upon issuance of the certificate

- Make warranties to persons using the certificate to verify digitally signed messages (Adams and Lloyd, 1999, p. 194)

3. Relying Party

A relying party is the user of a certificate (Austin, 2001). A relying party's obligations include:

- Verification of digital signatures from originating subscribers
- Knowledge of the rules associated with digital signature acceptance
- Record-keeping to help resolve any disputes that may arise in the future
- Understanding what to do when things go wrong, and/or when something occurs that requires the intervention or action of the relying party (Adams and Lloyd, 1999, p. 194)

B. DOD PKI USER ROLES AND RESPONSIBILITIES

The Department of Defense has defined similar roles for its PKI. The following sections describe the roles and responsibilities of users and entities within the DoD PKI.

1. Root Certification Authority

The Root Certification Authority (RCA) is the source of trust throughout all levels of the DoD PKI. The security of the RCA is paramount, as any compromise of the RCA would result in the compromise of the entire underlying PKI. In order to maintain this trust in the RCA and ultimately the entire PKI, the RCA must follow the DoD Certificate Practice Statement appropriate to the level of PKI the RCA is operating on. (DoD Class 3 PKI CONOPS, 1999)

The RCA is responsible for establishing subordinate Certification Authorities (CAs), establishing security policies for these CAs, generating and signing its own certificate, signing the certificates of its CAs, and revoking the certificates of any CAs if any degree of compromise is suspected. The RCA is also responsible for maintaining backups of all software, the certificate database, and private keys such that the RCA could be rebuilt in the event of a catastrophic failure. The RCA is responsible for ensuring that its subordinate CAs issue updated Certificate Revocation Lists before the current ones expire. (DoD Class 3 PKI CONOPS, 1999)

2. Certification Authorities

Certification Authorities (CAs) are established by and subordinate to the RCA. Like the RCA, they play a critical role in the overall trust of the DoD PKI, and they must conform to all applicable policies and regulations. The responsibilities of a CA are processing the registration of users, creating and signing user certificates, and maintaining CRLs. These tasks are accomplished by operating and maintaining a CA server, and conducting all aspects of certificate management – initial issue, reissue, revocation, re-keying, and updating CRLs. Additionally, like the RCA, each CA must maintain backups of software, the certificate database, and private keys in order to facilitate a rebuild in case of a catastrophic failure. (SPAWAR, 1999)

The CA is another vital link in the trust chain of the DoD PKI. The CA signs the certificates of its registered users, and the RCA signs the certificates of its established CAs. This allows the user to prove that he or she is a valid user of the PKI provided that the CAs certificate is valid and the RCA has not been compromised. (DoD Class 3 PKI CONOPS, 1999)

3. Registration Authorities

Registration Authorities (RAs) act as an interface between the CA and the subscribers. They are also responsible for following all applicable policies and regulations regarding the DoD PKI. RAs verify the identity of users requesting to be registered with a CA and to be provided with a public/private key pair. The RA may authenticate users within his or her organization. This responsibility of user authentication may be delegated to a Local Registration Authority (see section 4). RAs have two unique privileges. They can revoke any certificate within their organization, and they can revoke certificates of other RAs. (DoD Class 3 PKI CONOPS, 1999)

4. Local Registration Authorities

Local Registration Authorities (LRAs) exist to reduce the workload of an RA and to bring the PKI registration service closer to the subscriber. LRAs are appointed via requests to the PKI PMO. RAs will identify and authenticate an LRA using a government issued identification card. Large organizations may have many LRAs. These may be staff personnel with other primary responsibilities, or they may be full-time

LRAs. LRAs are also bound to the DoD PKI policies and regulations and must ensure that the users they are registering understand the responsibilities of possessing and using a DoD PKI certificate. LRAs pre-register users during a face-to-face transaction. After a user's identity has been verified, the LRA generates a Certificate Registration Instruction (CRI). The user follows the steps on the CRI, completes the registration process, and obtains his or her key pair and certificate. LRAs may revoke certificates as requested by a certificate owner or the organizations Information System Security Officer (ISSO) (see section C3 in this chapter). (DoD Class 3 PKI CONOPS, 1999)

5. Trusted Agent

The Trusted Agent (TA) is an optional role that may be assigned within the DoD PKI. The purpose of a TA is to help reduce the workload of the LRA. An LRA must make a request to the RA to appoint a TA. When a TA is in use, the LRA will generate a CRI for the user, the TA will perform the face-to-face authentication with the user, and the TA will distribute the CRI. A TA must sign a statement of agreement and understanding of responsibilities prior to performing these functions. (DoD Class 3 PKI CONOPS, 1999)

6. User

The majority of people within the DoD PKI will fall into the role of a User. The User role can be further divided into 3 sub-roles.

a. Subscriber

A Subscriber owns the public/private key pair and certificate. A subscriber may be a person or a machine. In the case of a machine, the administrator for the machine becomes responsible for the key pair used by the machine. A Subscriber uses the key pair to sign messages, encrypt/decrypt data, and authenticate themselves to other users. The identity of a Subscriber is bound to his or her private key (based on face-to-face authentication); therefore, the Subscriber must protect all private keys and passwords. The Subscriber is responsible for reporting any possible compromise to the RA as soon as it is suspected. The Subscriber's certificate contains identity information and the public key. This certificate is signed by the CA in order to carry on the trust link

all the way back to the RCA. This complete flow of trust from the RCA to the User is depicted in the following figure.

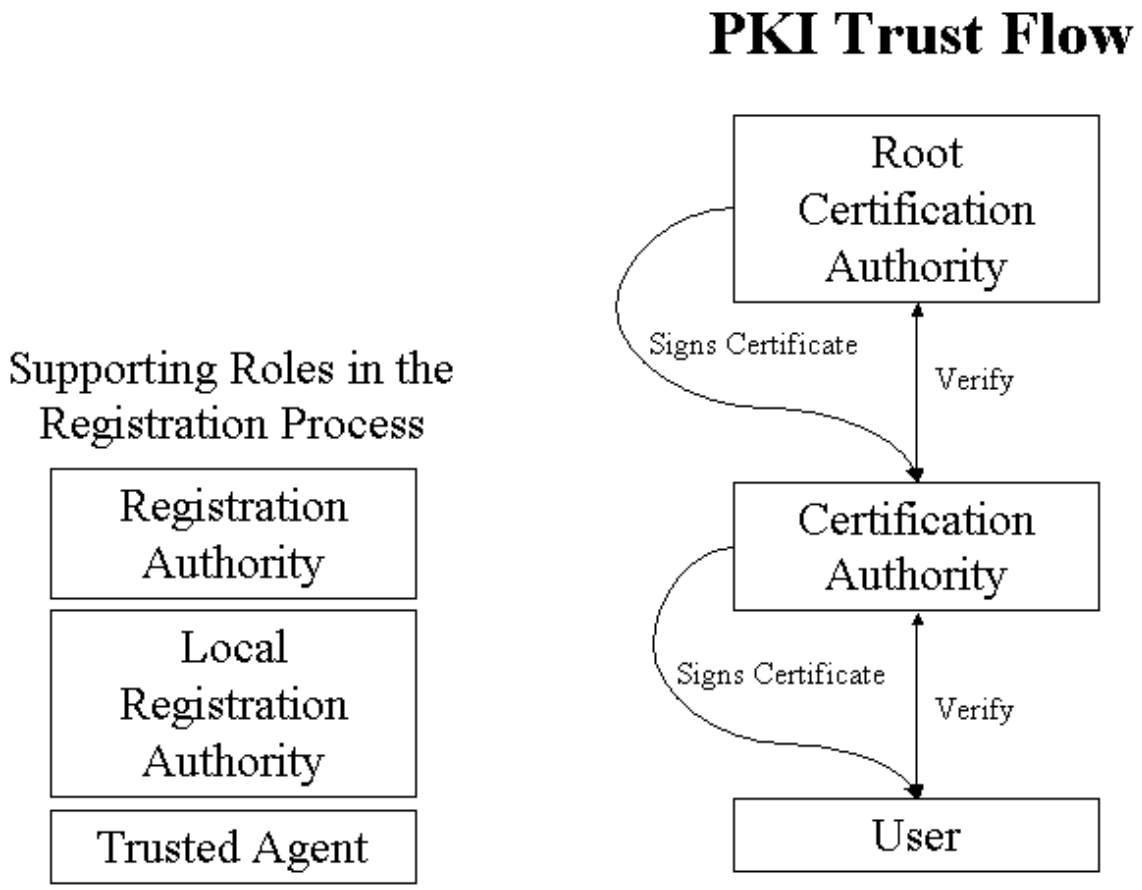

Figure 4.1 PKI Trust Flow

b. Relying Party

A Relying Party is the entity that uses and relies upon the binding of a person or component and their key pair. A Relying Party is responsible for validating the trust path from the user they are interacting with back to the RCA. This involves checking the current CRLs for all certificates in the path of trust to ensure they are all current and have not been revoked. (DoD Class 3 PKI CONOPS, 1999).

c. Directory User

A Directory User is someone who obtains information from a PKI directory about subscribers. This information may include public key certificates, organizations, phone numbers, and e-mail addresses. Most people who interact with a

PKI in any other role are often Directory Users as well. (DoD PKI Class 3 CONOPS, 1999)

C. ADDITIONAL DOD PKI ROLES

The user roles described in section B of this chapter are the most common roles that users of the DoD PKI will interface with directly. Other roles are less likely to impact the day-to-day user unless there is a problem with the PKI. These roles are described briefly in the following sections.

1. Directory System Administrator

The Directory System Administrator is responsible for maintaining the repository where users can obtain certificates and verify that they have not been revoked. The Directory System Administrator is responsible for maintaining a high level of availability, performing adequate backups, and managing appropriate access controls to ensure the integrity of the directory itself. (DoD PKI Class 3 CONOPS, 1999)

2. Archive Administrator

The Archive Administrator is responsible for the long-term storage of PKI materials. This includes properly storing the material, providing the necessary protection, and performing updates and media conversions as necessary. (DoD PKI Class 3 CONOPS, 1999)

3. Information Systems Security Officer

The Information Systems Security Officer (ISSO) is responsible for overall component security. There is one ISSO for the RCA workstation and each PKI server. The ISSO is responsible for making sure all policies and procedures are in place and followed, assigning privileges and access controls to CA accounts, reviewing the audit logs, and taking appropriate action in response to any suspicious activity or violation of procedures. (DoD PKI Class 3 CONOPS, 1999)

4. System Administrator

The System Administrator is responsible for the operations and maintenance of a PKI component. This includes configuration, installation, and recovery from failures. The System Administrator coordinates with the ISSO on all security issues and also

maintains backup files and off-site storage to ensure rebuild capability in case of a catastrophic failure. (DoD PKI Class 3 CONOPS, 1999)

The complexity of a PKI necessitates the various human roles and their related responsibilities. The people in these roles must understand what their responsibilities are and have the knowledge required to fulfill them. Chapter V will focus on the training requirements for the users of a PKI. Specifically, it will describe the need for PKI training within the DoD and suggest a potential method for delivering this training to the user.

THIS PAGE INTENTIONALLY LEFT BLANK

V. TRAINING FOR THE DOD PKI

The implementation plans and the identification of user roles within the DoD PKI are key components of its overall success. These define the framework within which operations will take place. Another key aspect of any shift in policy or practice is the human factor. The following quote from Austin reminds us that all components of a system must be taken into consideration. "Most important is the fact that with IT security, just as with military security or castle fortification, security is only as good as its weakest components." (Austin, 2001, p. 23-24) This chapter addresses the need for training of all personnel who will be using the DoD PKI. Without proper training, the integrity of the system as a whole will be in jeopardy.

A. THE TRAINING NEED

The decision of the DoD to implement a PKI as a part of its Defense in Depth for information assurance was only the first step. As the previous chapters have illustrated, a PKI is a complex environment that relies completely on the element of trust among all of its components. Without this trust, a PKI will not provide the services and levels of assurance that it is designed for. As with any environment or system that relies on the performance of all of its components, the system as a whole is only as strong, robust, or, in the case of PKI, as trustworthy as its weakest component. The integrity of a PKI must be supported by appropriate policies, technologies, and user behaviors. The policies and technologies are somewhat more static and controllable than the user behaviors. "Underlying a successful policy are *resources* to support enforcement, educate users, and modify the environment as external and internal conditions change." (Austin, 2001, p. 26)

As with the implementation of any new way of doing business, the resistance of people who must be involved in the DoD PKI will be the most difficult roadblock to overcome. The addition of the technological aspect to this change in business makes the task even more difficult. In order to implement and maintain a PKI that performs its intended functions, the users must be properly trained and monitored to ensure the trustworthiness of the PKI is not broken by their actions or inactions.

Training for the DoD PKI is not a small task. It is estimated that over three million certificates will be required for the DoD PKI implementation (Green, 2001).

Devising a method and delivering training to users of that many certificates is a complex effort. In addition to the sheer numbers involved, the level of knowledge and understanding about PKI that is desired is not something the average person has. Training must conform to a certain greatest lower bound of existing knowledge so as to not leave out those with limited technology backgrounds. The end users will not need the same level of knowledge as an LRA or RA, but they will still require a deep enough understanding of the PKI to recognize the impact that their individual actions will have on it.

B. CURRENT TRAINING EFFORTS

DoD personnel have a variety of PKI training materials available to them. There are multiple websites from which materials may be downloaded, viewed online, or ordered. The majority of these materials are text documents, slide presentations, interactive CD-ROMs, and video tapes. Some training courses for RAs and LRAs are offered. One of the largest Internet sources of PKI information is the Defense Information Systems Agency's (DISA) Information Assurance Support Environment (IASE) website (http://iase.disa.mil). This site provides links to general PKI information, training documents, and information on RA/LRA training courses offered by DISA. The RA/LRA course is currently only offered in one location, and the dates are limited. The training documentation includes guides for the end user, LRA, and RA.

Another source of PKI training is the Space and Naval Warfare Systems Command (SPAWAR). SPAWAR has a website that deals with the Medium Grade Services which is a Defense Messaging System level of service that is provided by combining class three DoD PKI and e-mail clients. This provides authentication and content integrity for the users of the messaging system. Although this training focuses on these Medium Grade Services, it does provide a basic overview of public key cryptography.

Part of the difficulty with DoD PKI training availability has arisen from the fact that the responsibility for this training is split. As mentioned earlier, DISA does provide a limited amount of RA and LRA training, but the responsibility for end user training rests with the individual services. Individual services do have some PKI training

available. This discussion will focus on the efforts of the United States Navy and Marine Corps. The Marine Corps utilizes the RA training provided by DISA and provides its own LRA training from their RA in Quantico, VA. The RA is also the focal point for end user training. The newest training available for end users in the Marine Corps is a computer-based training (CBT) PKI Overview Course that will be provided via CD-ROM. (Morris, 2001 (private communication))

The Navy also utilizes the DISA RA/LRA training courses and materials, and has developed "PKI 101" training on the basic concepts of PKI. According to Mr. Samir Othman, from the SPAWAR PKI Program Office, the Navy is taking an application-based approach to PKI training. Instead of developing and providing PKI training, they plan on adding PKI training to specific application training as the applications become PKI-enabled. The Navy currently has no plans to provide any additional standard PKI training. (Othman, 2001)

Although some DoD PKI training is available, there is not a single source that users can go to in order to obtain the training they require. The current PKI training development efforts are segmented and vary among the DoD components. This has led, and will continue to lead, to segmented, non-standardized training for users of the same PKI. Personnel in the Marine Corps will receive different training from personnel in the Navy and the Army, yet they will all be expected to interact with each other and follow the same basic rules when using the DoD PKI. Although some customization of training will be required based on the particular applications in use by a particular service or command, a more consistent, updated, centralized training effort would help ensure that all users of the DoD PKI are trained to a similar level and are able to understand and use the PKI effectively. Without this common understanding of all users, the trustworthiness of the PKI will be at serious risk.

C. A DOD PKI TRAINING FRAMEWORK

1. The Argument for Web-based Training

Before a discussion on the applicability of web-based training (WBT) to the problem of DoD PKI training can take place, a definition of web-based training must be provided.

> WBT is instruction that is delivered via a Web browser (such as Microsoft Internet Explorer or Netscape Navigator) through the Internet or corporate intranet. It offers online classes with facilities for interacting with a live instructor and other students or simply as independent study in which the student works on their own with, perhaps, contact through e-mail and real-time 'chat' with the tutor and other students. (Steed, 1999, p. 28)

In general, many benefits can be realized through the use of WBT. Steed (1999) discusses these benefits from two perspectives: 1) that of the user or manager, and 2) that of the WBT provider. From the user or manager perspective, WBT provides the following benefits:

- ***Reduced training costs per person*** – costs to deliver training are approximately 20-25% less than classroom delivery, and other indirect costs are saved as well (i.e. - travel, accommodations, etc.).
- ***Consistency of presentation*** – the same exact training is available to everyone.
- ***Up-to-date material*** – the most current training materials are available to all users. This is especially important for the Navy and PKI; the materials/technology change rapidly, and the students are numerous and geographically dispersed.
- ***Faster completion of training*** – studies show a 30-70% time savings in WBT over classroom training because students have more control over the learning environment
- ***Affordable technology*** – for the users, a connection to the Internet (or Intranet) and a computer with a web browser is all that is needed to access web-based training. The cost for these tools is small compared to the costs of travel and lodging for classroom training. Within the Navy, these tools already exist.
- ***Course management control*** – the training can be centrally maintained or have multiple control sites depending on the specific needs of the system. This includes controlling who is accessing the training and monitoring student progress
- ***Accessibility*** – web-based training can be accessible by anyone with a web browser and an Internet connection. This could include access from home as well as from the office or from anywhere in the world.

According to Steed (1999), WBT provides the following benefits from a provider perspective:

- ***Reduced training development costs*** – there are standard, platform independent tools available for web development.
- ***Distribution ease*** – this is done instantly via a web server and/or database server. A single installation or update provides the entire user community with immediate access to the update.
- ***Up-to-date content*** – as soon as the content is updated on the server, it is updated for all users.

Of course, there are some disadvantages to WBT as well. From a user, manager, or a provider perspective, Steed (1999) lists these disadvantages of WBT:

- ***New software and procedures*** – although the use of web technology has grown, some organizations may be providing training to individuals who are not familiar with web browsers and are not comfortable with web technology. Additionally, a switch from traditional classroom training to web-based training will require changes in training procedures (i.e. – applying for training, getting approval for training, and scheduling training). For Navy personnel, these concerns are not too great as there are already many areas where computer-based and web-based training are being used.
- ***Bandwidth limitations*** – variations in the speed of users' Internet connections and the capability of their physical link to the Internet may require limitations on the materials provided by a web-based training system. The use of large-sized elements (i.e. – large graphics or multimedia files) would degrade the quality of a user's experience unless they had a high-speed Internet connection. This issue must be taken into consideration when designing the system and creating the training elements.

Some additional disadvantages of WBT also include:

- ***No hands on aspect*** – lack of access to actual training systems (a PKI in this case) while completing training elements may be a disadvantage to some users. This problem exists in traditional classroom training as well, and it is only overcome by the use of a laboratory classroom environment.
- ***No one-on-one with an instructor*** – some web-based training systems incorporate real-time chat sessions or allow for e-mail communications between a instructor and the students. Use of these tools is an attempt to simulate the face to face aspect of traditional classroom training. This is helpful, but the PKI Training Framework presented later in this chapter does not initially include either of these features.

With so many benefits and few disadvantages, it may seem like WBT could be used for any type of training in any situation. This is not the case. Although the benefits are numerous, other factors must be considered before deciding to use WBT as a partial or complete solution to training requirements. At least four issues must be examined:

- ***Geographic location*** – "if your company is geographically dispersed, with many people to train, distributed learning is often a much more efficient approach to training." (Steed, 1999, p. 222)
- ***Size of audience*** – "…distributed learning will often be a more efficient method of reaching larger audiences, whereas instructor-led training may be more adequate for reaching smaller audiences." (Steed, 1999, p. 222)
- ***Dynamic information*** – "When training is of a dynamic nature, such as fast-changing methods, procedures or products, it is important that learners are kept up-to-date with the latest changes. In these situations, it may be more efficient to deliver incremental training using distributed learning." (Steed, 1999, P. 222)

- ***Timing of delivery*** – "When situations arise demanding rapid distribution of training, such as the release of new products, timing may be critical. In these situations, distributed learning is the most effective method." (Steed, 1999, p. 222)

An examination of these issues can be done regarding DoD PKI training. The DoD in general and specifically the Navy is, without question, geographically dispersed, and a large number of personnel will require DoD PKI training. These factors make distributed learning more efficient than instructor-led, classroom training. The DoD PKI employs technologies that continue to change and evolve. This results in a need for more timely distribution of new technological products and procedures. In this situation, distributed learning has the edge over classroom-based courses in the ability to delivery the most current information to students on a near real-time basis.

One may conclude that PKI training in the DoD is a prime candidate for a web-based delivery system. The current methods of providing PKI training to DoD users have many disadvantages that can be overcome by utilizing existing technology within the DoD. A user accessing training from his or her office overcomes the high cost of attending training courses. The existing access to the Internet as well as command and service intranets means that no additional investment in technological capability would have to be made in order to access online training resources. A more consolidated training resource would take the burden off of the users and save them the time and effort it takes to locate training from multiple sources. A centrally managed training source would also allow the most recent information to be available in the time it takes to update a database or a web page. The content of PKI training is amenable to the web as it is already delivered electronically in many cases. A web-based training framework for PKI would provide a more organized, more flexible method of obtaining the specific training required or desired by all DoD PKI users.

2. A PKI Training Framework

Based on the previous discussion, a web-based framework for DoD PKI training would improve the current state of this training effort. The remainder of this chapter will focus on the characteristics of such a framework. The detailed design information

presented in the following sections will be implemented into an actual training framework prototype.

As an overview, the proposed web-based PKI training framework has the following basic attributes:

- It would be centrally maintained. This attribute is critical for maintaining the most current, up-to-date training information available. Central management and maintenance is a key requirement. A logical candidate for this responsibility is the Root Certificate Authority or another designated office responsible for the overall training effort. If a single controlling entity is not an option, each component could manage their own training and maintain a central server containing the training framework and their own component-specific training. Due to the overlap of PKI training requirements between DoD components, a working group or task force made up of representatives from each component could be created to ensure information sharing and reduce duplication of effort. The maintenance issue is discussed further in section D.5 of this chapter.

- It would be accessible via a web browser through an Internet connection. The interface will be designed to function properly using the current versions of both Microsoft Internet Explorer and Netscape Navigator. Netscape Navigator is the browser required for downloading keys and certificates within the DoD PKI, and Internet Explorer is the standard web browser for the Navy.

- It would allow users to access training modules based on their role within the PKI (CA, RA, LRA, End User, etc.).

- It would allow users to access task-specific training to be used as a refresher or a type of help file.

These general attributes are applicable across the board for all users. There may, however, be circumstances in which each service, or individual commands may require additional flexibility in the way the training is presented. Although this potential need for

customization is recognized, the goal of this thesis is to design and develop the core framework only. As with any software system, upgrades and improvements are expected throughout its life cycle.

Another requirement for flexibility involves training for PKI-enabled applications. Different components and commands may employ numerous PKI-enabled applications. The users of the PKI training framework will need to be able to select from a variety of application-specific training modules. For example, numerous e-mail programs are in use within the DoD today. Training for all e-mail programs in use should be available within the training framework, and the user should be able to select the specific program for which he or she requires training. Eventually, the framework could be designed to allow individual components or commands to set up a specific profile that includes only command-specific PKI-enabled applications. This would filter the training available to users from a particular component or command. Either way, the user should have one address for the consolidated training that can then link them to service level pages with service-specific training, if this is a requirement. A drawback of service-level training pages is the maintenance and update of these pages. Another disadvantage is the potential for lack of consistency.

For the initial design, the goal of the training framework will be to accommodate all of the potential software options and facilitate the availability of training for each option. The user would be able to select from all of the available options.

D. PROTOTYPE DESIGN AND DEVELOPMENT

The DOD PKI training framework prototype involves two main components: a database and a web-based interface. The database will store information, and the web-based interface will display the information from the database as requested by the user. Although the specific details will be outlined in the following sections, there are some basic characteristics of a good web-based training program. Driscoll (1998) states that a well-designed web-based training program is interactive, has an easy-to-use interface, contains structured lessons, uses multimedia effectively, and pays close attention to both technical and educational details. A well-designed WBT also allows the user to have adequate control and freedom of movement within the site. The design of the DOD PKI

training framework will focus on the achievement of these goals with ease of use as a priority.

1. Goals and Required Functionality

The goal of the DoD PKI training framework is to provide a single method for delivering the most current PKI training to all DoD PKI users or potential users via a web browser and an Internet connection. The framework will serve all DoD personnel involved with the DoD PKI in any of the previously defined user roles. Because this group of people is large and diverse, the interface to the framework must be straightforward and easy to use with a minimum of basic computer skills. These basic computer skills include connecting to the Internet and using a web browser.

The framework will provide the following functions:

- The capability to search for training based on a particular user role (the prototype will only include the Registration Authority, the Local Registration Authority, and the User)
- The capability to search for training on a particular task or topic
- The capability to assess a user's knowledge of a particular training element (this aspect is a requirement, but will not be fully implemented in the prototype)
- The capability to track a user's completion of training elements (this will be linked to the assessment element)

The tracking capability is essential for management of users at the command level. Command or component policies will determine the specific training requirements for people serving in the various roles within the DoD PKI. For example, before being issued a key pair, an end user would be required to complete basic overview training and end user training. Requirements would also apply for RAs, LRAs, and all other user roles defined within the DoD PKI. Because the RAs and LRAs are responsible for issuing key pairs, they will need to have access to the training logs of their users.

2. Task List Development

A list of PKI tasks is required to provide the functionality listed above. For this prototype, a list of PKI tasks was developed using the existing training documentation as a guide. The specific documents used were the DISA trainee guides for RAs, LRAs, and Users, and the Marine Corps trainee guides for LRAs and Users (DISA, 2000) (United States Marine Corps, 2000). The task lists developed from these guides are contained in Tables 5.1, 5.2, and 5.3.

User Tasks
Obtain an identity certificate
Obtain an e-mail certificate
Find another user's certificate
Add a Netscape Communicator profile
Verify and copy certificates in the Netscape Personal Security Manager
Back up keys and certificates to a floppy disk
Delete a certificate from Netscape Personal Security Manager
Delete key3.db files in your profile directory
Import a certificate from a floppy disk
Download certificates
Determine which e-mail certificates you have
Send signed and encrypted e-mail
Receive signed and encrypted e-mail
Configure e-mail client

Table 5.1 User Task List

LRA Tasks
Add a Netscape Communicator profile
Install smartcard reader
Install smartcard software
Check the smartcard reader and token
Inititialize the smartcard
Change smartcard password
Change the token label
Request an LRA certificate
Import a certificate
Download, install, and configure the LRA workstation application
Move LRA encryption keys and certificate to the smartcard
Create a new user data file
Submit a user data file
Archive the user date file
Open and edit user data file
Re-enter users from the archive file
Import user data files
Print the user acknowledgement form
Send the RA the floppy containing the user data file
Attach a user data file to an encrypted e-mail message
Change the LRA settings
Access the LRA administration menu
Upload a user data file
Unlock a user account
Download the LRA application
Download the LRA release notes
Revoke certificate
Obtain server certificates
Find your LRA certificate
Search the CA servers

Table 5.2 LRA Task List

RA Tasks
Add a Netscape Communicator profile
Install the smartcard reader
Install the smartcard software
Check the smartcard reader and token
Initialize the smartcard
Change the smartcard password
Change the token label
Obtain the RA certificate
Move the RA encryption keys and certificate to the smartcard
Create LRAs
Revoke certificates
Update/Delete an entry on the directory server
Prepare e-mail certificates
Approve server certificates
Upload user data files from floppy disk
Search the CA servers
Find your RA certificate

Table 5.3 RA Task List

3. Database Design

The underlying database for the training framework is a key component of its overall design and functionality. The database will contain tables of information and documents that will be accessed by the users via a web-based interface. The database design must provide the capability to fulfill the functional requirements stated previously. This section will present the design details of the PKI training database. Those readers not familiar with the various models and tables presented may refer to Appendix A for additional information.

a. General Description

The PKI training database will store all of the information required for the training framework. This includes information on PKI user roles, PKI tasks, PKI training framework users, PKI training elements, PKI training evaluation elements, and individual user PKI training records. Additionally, information on each DoD component will be included. This information will allow for future modifications regarding component-level customization of the training framework. The PKI user roles will be used to customize training based on a particular user role. The PKI tasks list will allow users to

obtain training for a specific task only. Information about each user will provide the capability to track his or her training and evaluation progress. The PKI training elements are the actual training files. The PKI evaluation elements provide an evaluation of a user's grasp of a particular PKI training element. PKI training records contain the evaluation results for each user.

The training record for each user will track only the evaluation elements that have been completed by the user. This will provide confirmation of completion of any required training prior to the issuance of a PKI certificate, or the assumption of other roles within the PKI. Users will be able to access all available training at anytime for the purposes of refreshing their knowledge or obtaining new information that has become available. Any requirements and time intervals for this kind of refresher training should be determined at the component or command level and should be based on PKI roles. The framework would allow for tracking this refresher training only if the user completed the evaluation element(s) corresponding to the refresher training element(s). As refresher training requirements are established, the framework could be modified as necessary to accommodate additional tracking mechanisms.

The following sections detail the specific design of the tables and fields within the PKI training database. These models will be used as the basis for the prototype PKI training database.

b. Database Schema

The following is a schema of the PKI training database. A database schema defines a database's structure, tables, and relationships. It lists each table (in all capital letters) followed by a list of the fields contained within that table. A field underlined and listed in bold font is the primary key for that table. If multiple fields are underlined and listed in bold, they comprise a composite primary key for the table. A field name followed by "_FK" indicates a field that is a foreign key or the primary key from another table. The presence of this key indicates a relationship between the tables.

USER ROLE (**UserRoleID**, UserRoleName)

USER ROLE TRAINING ELEMENT JOIN (**UserRoleID_FK**, **TrainingElementID_FK**)

USER (**SSN**, LastName, FirstName, MiddleInitial, Password, ComponentCode_FK)

TRAINING RECORD (**DateCompleted**, **Result**, **SSN_FK**, **EvaluationElementID_FK**)

TRAINING ELEMENT (**TrainingElementID**, TrainingElementDescription, TrainingElementFileName)

TASK (**TaskID**, TaskDescription)

TASK TRAINING ELEMENT JOIN (**TaskID_FK, TrainingElementID_FK**)

TASK USER ROLE JOIN (**TaskID_FK, UserRoleID_FK**)

EVALUATION ELEMENT (**EvaluationElementID**, EvaluationElementFileName, TrainingElementID_FK)

COMPONENT (**ComponentCode**, ComponentName)

COMPONENT TRAINING ELEMENT JOIN (**ComponentCode_FK, Training ElementID_FK**)

c. Semantic Object Model

Figure 5.1 is a semantic object model for the PKI training database. This model depicts each table as an object. Within the object box for each table are all the fields contained within the table. Where relationships exist between tables, each one is included with the fields of the other. Fields preceded by two asterisks and listed in bold

font are the primary keys for their respective tables. The numbers after each field indicate minimum and maximum cardinality.

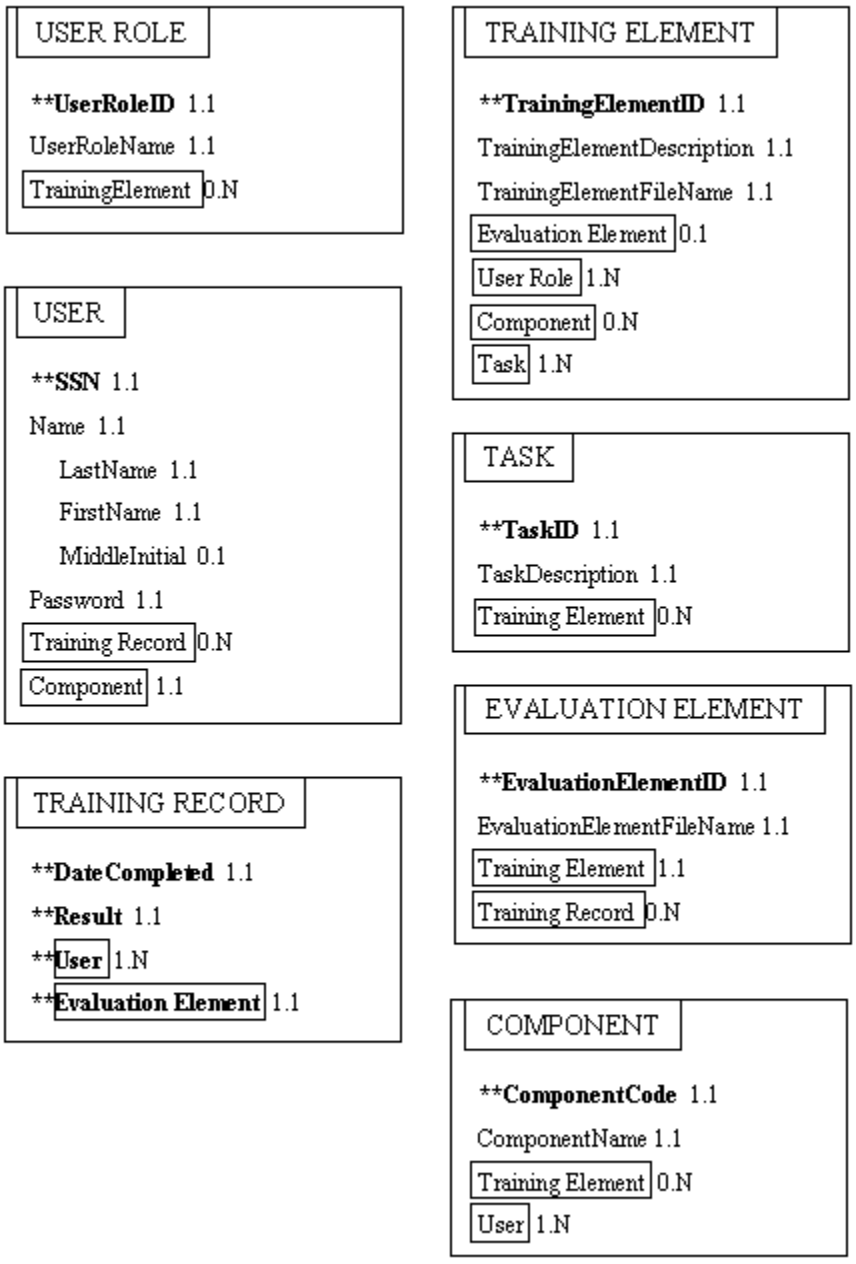

Figure 5.1 PKI Training Database – Semantic Object Model

d. Metadata

The following tables provide the metadata for the PKI training database. Table 5.4 is the metadata for the tables, and Table 5.5 is the metadata for the fields.

Table Name	Number of Fields	Primary Key
Component	2	ComponentCode
Component Training Element Join	2	ComponentCode_FK, TrainingElementID_FK
Evaluation Element	3	EvaluationElementID
Task	2	TaskID
Task Training Element Join	2	TaskID_FK, TrainingElementID_FK
Task User Role Join	2	TaskID_FK, UserRoleID_FK
Training Element	4	TrainingElementID
Training Record	4	DateCompleted, Result, SSN_FK, EvaluationElementID_FK
User	6	SSN
User Role	2	UserRoleID
User Role Training Element Join	2	UserRoleID_FK, TrainingElementID_FK

Table 5.4 Table Metadata for the PKI Training Database

Field Name	Table Name	Data Type	Length	Description
**ComponentCode	Component	Text	5	A unique ID for a component
ComponentName	Component	Text	50	The name of the component
**ComponentCode_FK	Component Training Element Join	Text	5	A unique ID for a component
**TrainingElementID_FK	Component Training Element Join	Long Integer		A unique ID for a training element
**EvaluationElementID	Evaluation Element	Long Integer		A unique ID for an evaluation element
EvaluationElementFileName	Evaluation Element	Text	50	The file name for the evaluation element
TrainingElementID_FK	Evaluation Element	Long Integer		A unique ID for a training element
**TaskID	Task	Long Integer		A unique ID for a task
TaskDescription	Task	Text	100	A short description of a task
**TaskID_FK	Task Training Element Join	Long Integer		A unique ID for a task
**TrainingElementID_FK	Task Training Element Join	Long Integer		A unique ID for a training element
**TaskID_FK	Task User Role Join	Long Integer		A unique ID for a task
**UserRoleID_FK	Task User Role Join	Text	5	A unique ID for a user role
**TrainingElementID	Training Element	Long Integer		A unique ID for a training element
TrainingElementDescription	Training Element	Text	50	A short description of a training element
TrainingElementFileName	Training Element	Text	50	The file name for the training element
**DateCompleted	Training Record	Short Date		The date an evaluation element was completed
**Result	Training Record	Text	4	The result of an evaluation element, "Pass" or "Fail"
**SSN_FK	Training Record	Text	11	Social Security Number of the user
**EvaluationElementID_FK	Training Record	Long Integer		A unique ID for an evaluation element
**SSN	User	Text	11	Social Security Number of the user
LastName	User	Text	50	User's last name
FirstName	User	Text	50	User's first name
MiddleInitial	User	Text	1	User's middle initial
Password	User	Text	20	User's password to login
ComponentCode_FK	User	Text	5	A unique ID for a component
**UserRoleID	User Role	Text	5	A unique ID for a user role
UserRoleName	User Role	Text	50	The user role title or name
**UserRoleID_FK	User Role Training Element Join	Text	5	A unique ID for a user role
**TrainingElementID_FK	User Role Training Element Join	Long Integer		A unique ID for a training element

Table 5.5 Field Metadata for the PKI Training Database

e. Relationship Diagram

Figure 5.2 is a relationship diagram for the PKI training database. This figure shows the links between the tables of the PKI training database and how they relate to each other.

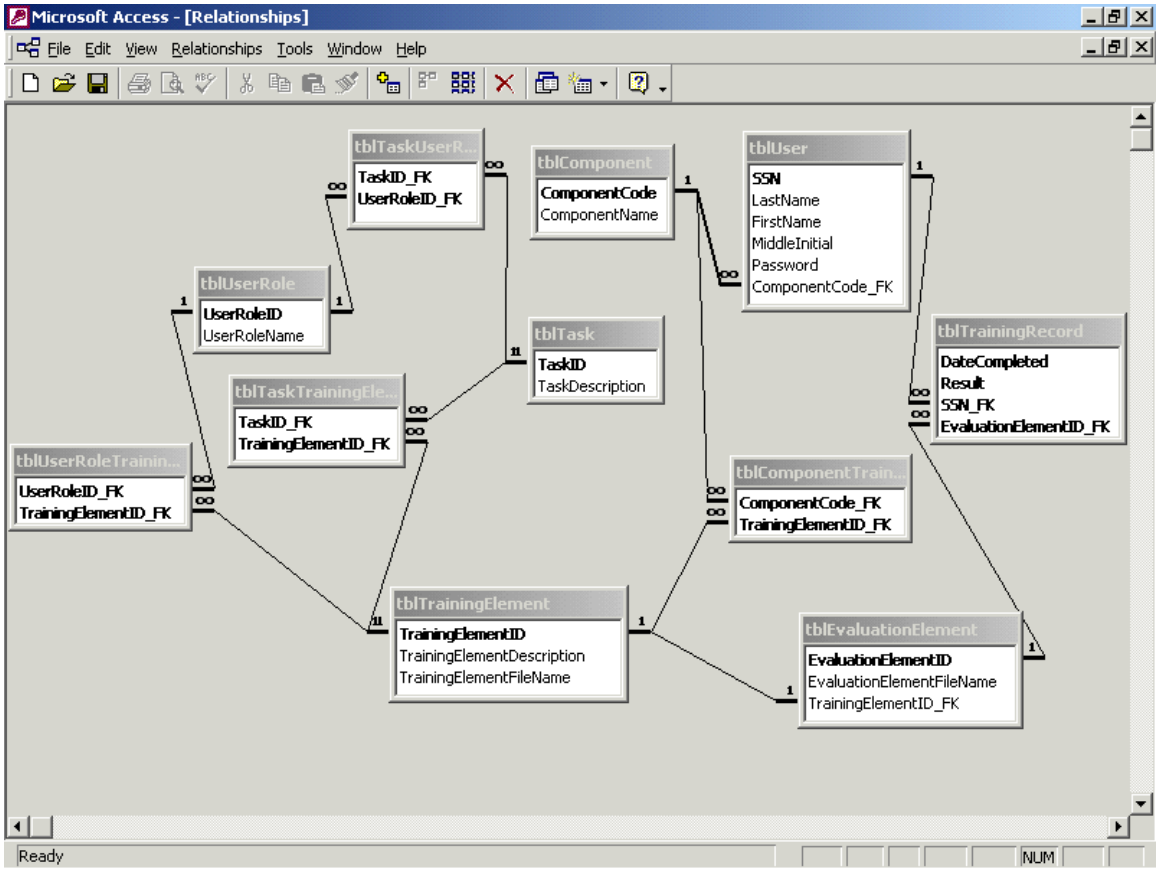

Figure 5.2 PKI Training Database – Relationship Diagram

4. Interface Design

a. Design Process

Designing an effective web interface involves several steps. Lynch and Horton (1999) identify six major stages of web site development: 1) site definition and planning, 2) information architecture, 3) site design, 4) site construction, 5) site marketing, and 6) tracking, evaluation, and maintenance. The development of the DoD PKI training framework in this thesis will proceed through stage two and move into stage

three with the development of a prototype system. The remaining stages will not be addressed, but they are potential areas for follow-on work.

Site definition and planning involves defining the goals, objectives, scope, and functionality of the site (Lynch and Horton, 1999). These elements have been defined earlier in this chapter. In summary, the DoD PKI training framework must provide the most current PKI training to all potential DoD users via a web browser and an Internet connection. The framework will allow users to search for training based on a specific role or a specific task. Users will be evaluated upon their completion of training elements, and a training record will be maintained for each of them.

Information architecture involves determining the details and the organization of the content of the site (Lynch and Horton, 1999). The bulk of the content of the DoD PKI training framework will be training elements and their corresponding evaluation elements. This information may be presented in a variety of formats, and the goal of the framework is to accommodate as many formats as possible. The most important aspect in this stage is the organization of the site. The way a user is allowed to navigate through the site should be flexible enough to allow him or her to obtain the desired information efficiently and directly. The user should be able to find the desired information with the fewest mouse clicks possible. The appropriate search tools must be available, and the user must never feel lost within the site. The specific flow and design of the DoD PKI training framework is provided in the following sections. The information architecture stage is also the time during which prototypes should be built. This will allow for the testing of navigation through the site as well as obtaining feedback on the overall design of the interface (Lynch and Horton, 1999).

The site design stage involves detailing the overall design of the pages, generating the content and the code, and completing all the components so they are ready for the construction stage (Lynch and Horton, 1999). Although this thesis will include the development of a prototype (information architecture stage), it will also include the design of the high level pages of the site. This will provide a starting point for actual user testing and modification of the existing interface. The framework will only be populated with a sampling of data to show functionality and allow for user feedback on the

navigational and design features of the site. Essentially, the prototype framework will be an initial, small-scale implementation to show the desired functionality and allow for testing and future revisions.

b. Web site hierarchy

The DoD PKI training framework web interface will begin with a "Login" page. This is where existing users can login, and new users can register with the system. Having users authenticate with a password at the beginning of the session will accomplish two main goals. The first is to verify the user's identity for the purposes of allowing him or her to access training records or complete evaluation elements. The second is to prevent non-registered users from accessing the training data and potentially slowing down access for those who are registered users.

After entering valid credentials, the user will be taken to the main navigation page of the site from here on out called the "Home" page. This page will contain the main navigational elements of the site. Users will be able to access "Training" (via various search methods), complete "Evaluations", view their "Training Record", or "Logoff" the system. Additional options will include a frequently asked questions or "FAQ" page, a "Feedback" page, a "Help" page, and a "Contact Us" page. All of these links will be contained in a contents frame of the "Home" page. These links will be available from any page within the site except those pages that are displayed in a new window. Pages designed to be displayed in a new window include the display of training elements and completion evaluations selected by the user. When a user selects the "Logoff" option, he or she will be given the option of logging off or returning to the "Home" page. These will be the only two options from the "Logoff" page. A general flow diagram of the web interface pages is included as Figure 5.3.

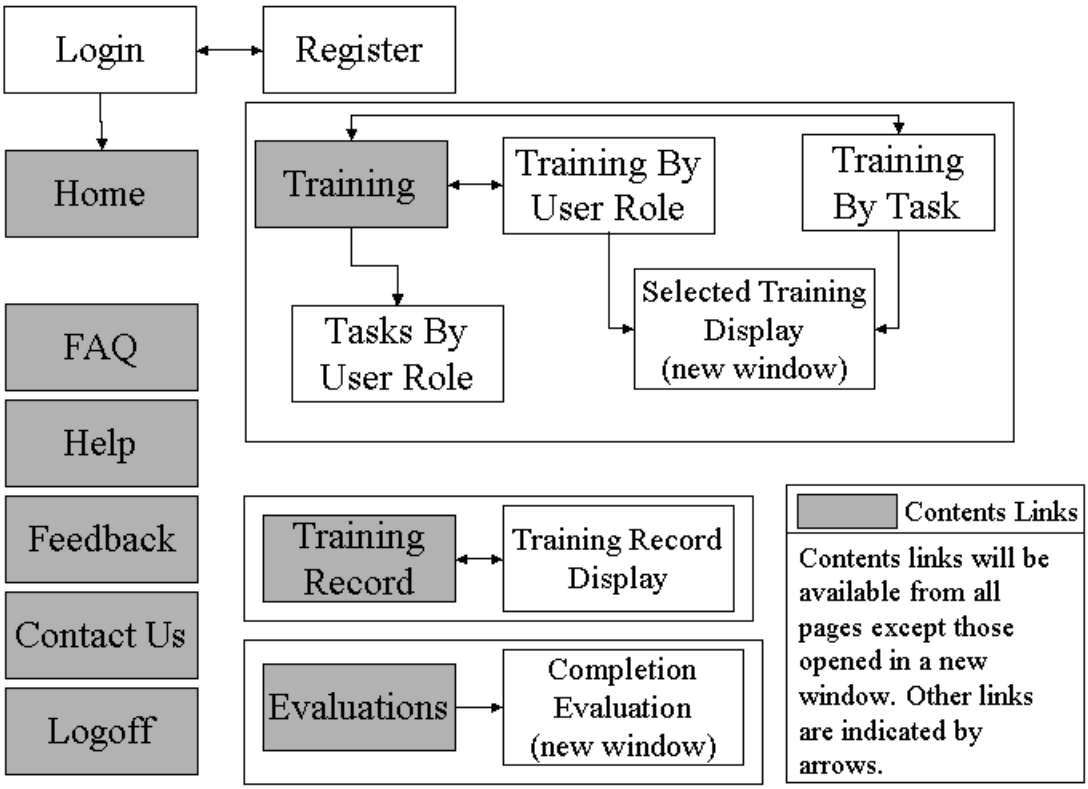

Figure 5.3 DOD PKI Training Framework - Interface Flow Diagram

Regarding the training and evaluation elements, links to these items will be presented to users within the main organization of the page. If they want to view or download items, new windows will be displayed. This will allow the users to keep their place within the primary framework and come back, from the new window, at any time during their view or download session.

c. Page layout and design

To fulfill the goal of allowing the users to access the information they desire with the fewest number of mouse clicks, a frames-based design will be used. Specifically, the interface will consist of three frames: a header frame, a contents frame, and a main frame. The layout of these frames is presented in Figure 5.4 below.

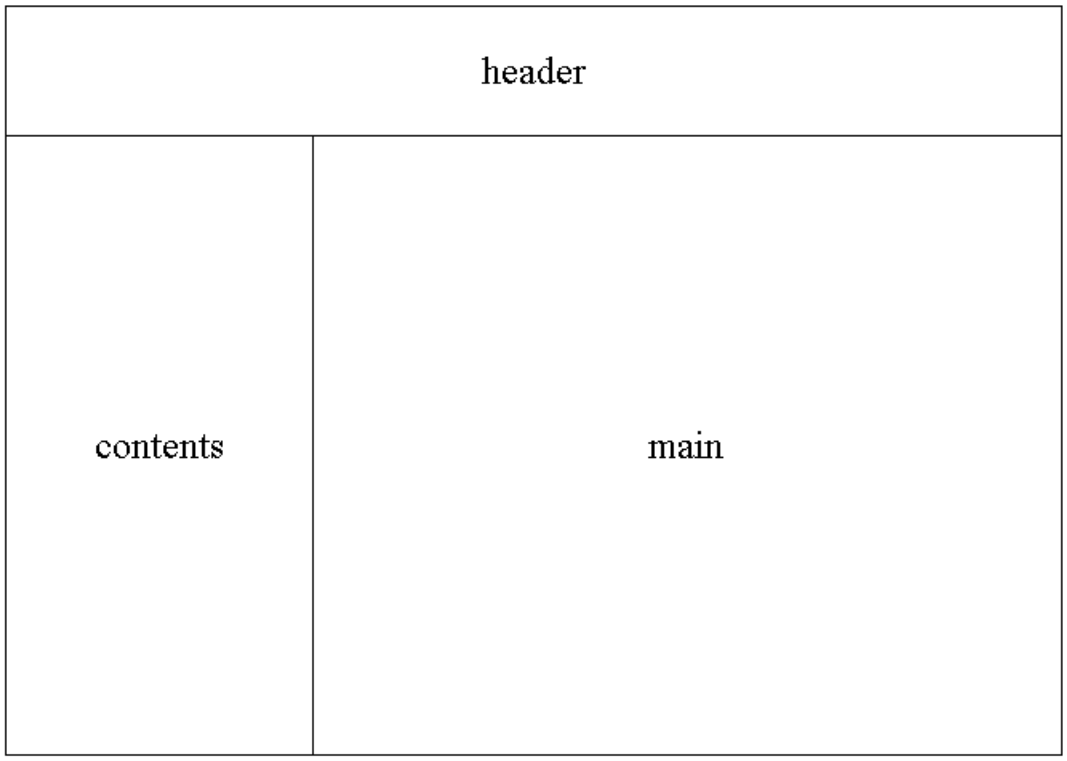

Figure 5.4 DOD PKI Training Framework – Frame Layout

The header frame will contain the title of the site, and the name of the user who is currently logged in. The contents frame will contain the navigational links for the site. These links are Home, Training, Evaluations, Training Records, FAQ, Help, Feedback, Contact Us, and Logoff. The main frame will contain the content selected by the user. Initially, the main frame will contain a welcome page that briefly describes the site and lists the overall point of contact for the site.

The majority of the content selected by users will be displayed in the main frame, and the header and contents frames will be static. The exception to this will be when the user selects a link to a specific training or evaluation element. These items will be displayed in a new browser window. The existing framework window will remain open to allow users to return to the framework at any time. Additionally, when a user selects the "Logoff" option, the logoff page will appear in the full window, and the header and contents frames will no longer be displayed.

The site will contain numerous HTML (hypertext mark-up language) and ASP (active server pages) pages. The html pages will present basic text information and navigational links. The active server pages will provide the link to the DoD PKI Training database. These pages will provide result sets from queries entered by users. The distinction between these pages will be essentially seamless to users, and their ease of use will be maximized. Table 5.6 below contains a listing of all of the pages that will comprise the site and their file names.

Page Description	File Name
Login page	index.htm
Registration page	registration.asp
Registration Confirmation page	register_confirm.htm
Login processing page	login.asp
Login Error page	login_error.htm
Footer Information page	footer_include.htm
Home page (frameset page)	home.htm
Contents page (lefthand frame contents)	contents.htm
Welcome page (initial main frame contents)	welcome.htm
Header page (header frame contents)	header.htm
Training Element home page	training.htm
Training Element Search by User Role page	train_user_role.asp
Training Element Search by Task page	train_task.asp
Task Search by User Role page	tasks_user_role.asp
Evaluation Element home page	evaluation.asp
Training Records home page	training_record.asp
Contact Us page	contact.htm
FAQ page	faq.htm
Feedback page	feedback.htm
Help page	help.htm
Logoff page	logoff.htm
Logoff processing page	logoff.asp

Table 5.6 DOD PKI Training Framework – Interface Files

In addition to the layout, the site will utilize a standard font and color scheme to ensure consistency throughout all of its pages. The exception to this will be the training and evaluation elements. Since one of the goals of the site is to accommodate multiple types of training elements, it is assumed that the elements will be designed and presented in various formats with various design techniques. The

standardization of the training and evaluation elements is beyond the scope of this thesis and is a good topic for further research and development. The potential for variation in the training and evaluation elements is more support for having them displayed in new windows separate from the training framework itself.

Graphic elements and special text features that greatly increase the size of the interface files will be avoided. The framework can perform the required functions with a minimal use of these items. The training elements may contain larger files or special presentations (such as audio or video files), but these larger items can be downloaded and studied offline. The only danger with this practice is that the information may be updated and the user may be holding on to an old file. Requiring that all elements within the site, including all training elements, have an accurate date stamp to inform the user of the last time the item was updated will ease this potential problem. A simple comparison of the dates will let the user know if he or she is holding the most current version of an element.

Some specific details regarding the prototype design are provided in screen shots contained in Appendix B of this thesis. As previously stated, this prototype is intended to serve as a starting point for user testing, further requirements definition, and improvements in design and functionality. Scalability is also an issue that must be accounted for when a system like this is to be deployed DoD-wide.

5. Maintenance and Control

In order to ensure that the most up-to-date training is available and that all users have access to the same training, the content of the PKI training framework must be centrally controlled and maintained. Because the training for the DoD PKI has been pushed down to the component level, there is currently no central point of contact or central office of responsibility for training at the DoD level. In order for the web-based PKI training framework to be effective, it must be controlled at this level, or delegated as a whole to a specific component or program office. Several options exist within the current DoD PKI organizational structure.

The first option is that the DoD PKI Program Office take control of the training task. They are the central point of contact for current DoD PKI issues. Since all

implementation and policy guidance flows down through this office, they would be a logical choice to control the training that is being developed and maintain the training available to users via the PKI training framework.

Another option is to select a DoD PKI Certificate Authority to take over the training task. This is not an ideal situation as the CA is already tasked with all of the CA responsibilities, and they may not have the required expertise to guide the development and maintain the content of the training framework.

A third option is to delegate the PKI training for all of DoD to one component. The Navy, Marine Corps, Army, or Air Force could be tasked with the development and maintenance of all DoD PKI training including the maintenance of the training framework. A problem with this option is that each component may have different applications in use and different PKI implementations. If one component was in charge of the PKI training task, they could not perform this duty in a vacuum. Coordination between PKI representatives from each DoD component would be required on a regular basis to ensure that the interests and training needs of each were being addressed. With one component ultimately in charge, friction may develop between them and the other components involved.

Because of the scale and importance of the DoD PKI training effort, it is highly recommended that it be handled at the DoD level. All components and commands involved with the DoD PKI would be involved in the development of specific training elements, but the overall control and maintenance of the training system would be done at a higher level. This would ensure that all components' needs are being met, and that all DoD PKI users have access to the most current training information and materials available.

Several obstacles to implementing this high level of control exist in the current environment. The two most important issues are 1) the focus of the PKI PMO on higher level policy and implementation issues and their organizational distance from the intended recipients of the training, and 2) the existing efforts that have been made by individual components regarding PKI training. The Navy and the Marine Corps have some existing training procedures in place, and, replacing these with a centrally managed

training framework developed with little or no involvement by the services could have a detrimental affect on morale and decrease the commitment to the training and PKI in general. A potential solution is the implementation of the proposed training framework at the component level while ensuring coordination and communication between all components involved. The framework could be provided as a tool and a delivery method for the existing training within each component. This would allow for the distributed approach to some of the more basic level PKI training while leaving more advanced training, such as RA and LRA training, to the traditional classroom setting. Components would have a significant amount of control over their piece of the framework, but they would be able to access contents provided by other components as well. This idea conflicts with the requirement for a centrally managed and maintained framework, but is a more workable, realistic option that will begin to push the training effort in the right direction.

E. TRACKING THE TRAINING

Once a viable DoD PKI training system is implemented, tracking individual training will become an important task. The best way to handle this tracking is to build the functionality into the training system itself. The PKI training framework prototype is designed with this in mind. The PKI training database contains a table called 'TRAINING RECORD' which will contain information about users and the training elements they have completed. The link between the user and the completed training elements will be made through evaluation elements. These will be evaluation or assessment tools that will be developed for each of the training elements or groups of training elements. After completing a training element or set of training elements, a user would proceed to the corresponding evaluation element. The developer of the training and evaluation elements would determine the criteria for passing the element. The user would complete the evaluation element and the result would be stored in the 'TRAINING RECORD' table as an instance of a training record for that user, for the specific training element.

In addition to this automated tracking, components or commands will need to institute policies and procedures that will ensure that users do not use PKI-enabled applications for which they have not been trained. This may be best accomplished by

providing the necessary impact with the basic training that is required prior to receiving a PKI certificate. Users at all levels must have a clear understanding of the impact their actions may have upon the PKI as a whole. This understanding is best reinforced through the attitudes and actions of other PKI users and especially those in positions of greater responsibility (i.e. – RAs and LRAs).

Because these training records will contain personal information about individual users and their performance on the evaluation elements, the access to these records must be protected. The users themselves will be required to select a password to access the training system as a whole. This password will allow users to view their own personal training records. Additionally, there may be a need for LRAs or RAs to have access to the training records of the End Users they register with the DoD PKI. This would allow the LRA or RA to verify that End Users who apply for a certificate have completed any required training. These requirements should be developed at the DoD level to ensure that the appropriate levels of training are being completed by End Users throughout the DoD. Individual components should be allowed to modify the DoD PKI training requirements only to make them more strict or require training over and above that required by the DoD. The verification that any required training was completed should then be a standard step in the DoD PKI registration process.

As new PKI-enabled applications are brought online, existing users should be notified and instructed to complete the required training for the applications prior to using them. It is not desirable or feasible to revoke and reissue certificates to users each time a new PKI-enabled application is installed. Once again, the importance of proper behaviors and adherence to procedures regarding the PKI must be emphasized in the initial basic PKI training and reinforced through command climate and leadership of other PKI users.

The implementation of any new technology requires some degree of training for the users. With the DoD PKI, the requirement for training of its users is extremely great. The nature of the DoD PKI is such that it relies heavily on the trust within the system. The fastest way to destroy that trust is to unleash untrained, ignorant users on it. Because this training is vital to the successful use of the DoD PKI, the author believes that a

segmented, distributed approach is not ideal. The author does however; recognize the potential difficulties of implementing the proposed framework at the DoD level. The potential implementation of this training framework at the component level with overall coordination and communication between components would be a more realistic step toward improving the existing training efforts. Potential users of the DoD PKI need a consistent, up-to-date, user-friendly method of obtaining the appropriate training for their potential role within the DoD PKI. Web-based training has been shown to be an efficient, effective method of delivery in similar circumstances. The prototype PKI training framework will provide the basic structure within which DoD PKI training can be housed and distributed to those who need it.

THIS PAGE INTENTIONALLY LEFT BLANK

VI. CONCLUSIONS

The concept of a public key infrastructure in itself is not an easy one to master. Adding the existing complexities of the DoD (i.e. – numerous components, large numbers of organizations, cultural diversity, wide range of existing technology) makes the implementation of a PKI an even more daunting task. Given the need for the added security that a PKI can provide, implementation of the DoD PKI is still a task that must be faced. This thesis has presented a basic overview of the PKI technology and has highlighted the need for all users within a PKI to be trained appropriately. The PKI training framework was developed as a tool to assist in fulfilling this massive training requirement within the DoD. The framework and prototype developed by the author is however, only the beginning. The following paragraphs outline potential follow-on work related to this thesis and additional related areas for future research.

A. THE DOD PKI TRAINING FRAMEWORK

This thesis provided an initial prototype of the proposed DoD PKI training framework. This is only the beginning of what will need to be accomplished in order to make this framework a reality within DoD. The work presented in this thesis should be continued with testing of the prototype to 1) identify additional requirements, 2) define areas where it is lacking in required functionality, and, perhaps most important, 3) ensure its usability. While the interface is being tested and improved, there must also be an effort to develop the training and evaluation elements that the framework will contain. This effort will most likely involve people and organizations throughout the DoD. The framework itself will only be as useful as the content it contains. A mechanism to identify, develop, and review the needed training and evaluation elements must be implemented.

The control of the training framework and its content is also a key issue that will require further investigation. The control and management options presented in this thesis are just that, options. Additional organizational research within the DoD is needed to determine the most effective level of control and management for a system like the DoD PKI Training framework. The advantages and disadvantages of each possible scenario should be analyzed with regard to the overall goal of the framework and the PKI

training effort as a whole – providing the right training to the right people at the right time to minimize the risks of violating the trust required within the DoD PKI.

Other issues specific to the proposed framework include expanding the tracking portion of the system to better accommodate the tracking of refresher training. This will be an important requirement as the DoD PKI grows and matures. More certificates will be issued, and more PKI-enabled applications will be installed causing the need for new and refresher training to be ongoing.

Finally, based on the level of implementation and the level of control of the training framework, it will need to be developed as a more robust system. The prototype was developed as a proof of concept and a demonstration of the planned interface. The underlying database will need to be built using enterprise-level software and maintained on hardware capable of handling the amount of use that is expected. As with any system, appropriate plans for mirroring, backups, and security will need to be developed and implemented. As was stated previously, the development of the initial prototype was simply a first step.

B. ADDITIONAL AREAS FOR FUTURE RESEARCH

In addition to the follow-on work involving the training framework, there are related issues that, with further research, could prove beneficial to the DoD PKI. Some of these areas are listed below.

- The identification of required training elements for each role within the DoD PKI. This would set the minimum standard for an individual to meet prior to assuming any role within the DoD PKI.
- The identification of refresher training requirements. This would include the timing and content requirements of refresher training.
- The development of procedures to ensure proper training for new PKI-enabled applications is completed prior to the use of these applications. The overall PKI must have checks and balances that will provide for an adequate level of assurance that users will not perform functions using PKI-enabled applications for which they have not been trained.

- The development of some type of 'emergency procedures' for DoD PKI users. These would provide assistance to users who discover a potential or an actual breach in the trust of the DoD PKI either through user actions or system errors or failures. For example, these procedures would provide specific instructions to a user who discovers that his or her PKI certificate-containing token has been lost.

These additional aspects of training for the DoD PKI are necessary to provide as close to a complete training solution as possible. While there may always be a need for face to face, classroom training, it is this author's opinion that the timely, distributed nature of a web-based training framework can fulfill a large portion of the training need in the case of the DoD PKI. As with the PKI itself, this training tool must also be implemented properly in order to achieve its desired goals. By leveraging existing technology, and forming a more coordinated effort, the DoD can enhance the success of its PKI by providing more up-to-date and timely training to its current and potential users around the world. As the DoD becomes more and more "joint", the concept of a more centralized effort may become more of a reality. Until then, any step closer to that reality will be a positive one.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX A. DATABASE DESIGN AND MODELING

This appendix presents a brief introduction to database design and modeling. It includes database basics and a description of some database models – specifically those used in designing the PKI training database. This information was adapted from Kroenke, 2000.

1. DATABASE BASICS

A database can be described as a "…self-describing collection of integrated records" (Kroekne, 2000, p. 569). Databases are typically made up of tables or relations, fields or columns, and records or rows. A relation is a two-dimensional table that is comprised of fields and records. The columns of the table comprise the fields, and the rows of the table comprise the records. Each record in a table must be unique. To facilitate this, each table contains a field that is designated as a primary key for the table. A primary key must be a unique value that is never repeated within the table. The primary key is typically some kind of identification number or serial number. If the data being stored does not have a clearly identifiable, unique value associated with it, an additional field can be added to provide this unique key (i.e. – an auto-numbering field that assigns a unique number to each record as it is added to the table).

Tables typically contain related information. For example, a table named 'Student Info' may contain a student's name, identification number, address, phone number, and grade level. Another table named 'Course Schedule' may contain the names of courses, the time each course is offered, and how many students are enrolled in each course. If desired, a link between these tables could be created to facilitate the creation of a course schedule for each student.

When designing a database, the requirements must be clearly understood. These requirements most often involve the presentation of certain information in a particular manner. In order to effectively design a database to meet the requirements, an accurate database model must be developed. This database model provides the link between the requirements and the actual building of the database. A database model identifies what must be stored, the structure of the storage, and the relationships among the stored data.

Numerous modeling techniques exist. The following sections will describe the database schema, the semantic object model, and database metadata.

2. DATABASE SCHEMA

A database schema defines the database and provides the design by which the database is built (Kroenke, 2000). A schema includes table names, primary keys, and field names. The schema is organized by table, with the fields of the table following. Consider the following example:

TABLE NAME (**PrimaryKeyField**, Field2, Field3, Field4_FK)

The primary key field is underlined and in bold font. In some cases, multiple fields may be used together to form the primary key. In that situation, all fields comprising the key would be underlined and in bold font. The last field listed in the example ends in 'FK'. This indicates that this field is a foreign key in the table. A foreign key is a field "…that is a key of one or more relations (tables) other than the one in which it appears" (Kroenke, 2000, p. 573). Foreign keys are placed in tables to enable relationships between them.

A complete schema for a database will identify the tables, fields, and the basic relationships that exist between the tables. This is a good start, but a Semantic Object Model provides even more information.

3. SEMANTIC OBJECT MODEL

A Semantic Object Model (SOM) is one method of creating a database model based on what is to be stored, the characteristics of these things, and the relationships between them. In a SOM, the items to be stored or represented are called semantic objects. A more formal definition of a semantic object is a "…named collection of attributes that sufficiently describes a distinct identity" (Kroenke, 2000, p. 74). *Semantic objects* are grouped into *classes* and named to correspond with what they represent. Using the PKI training database as an example, one class or group of objects is called 'USER ROLES'. The *attributes* or *fields* contained within this class describe each distinct user role that is represented in the database. The class names are spelled with all capital letters. A specific user role within this class is called an instance of the class. For

example, ‘Certificate Authority’ is an instance of the class ‘USER ROLES’. The identification of the classes is the starting point for a SOM.

Once object classes have been determined, the attributes of these classes are listed. Attributes provide further definition of a class. Three types of attributes exist. *Simple attributes* have a single value such as date, social security number, or training element ID. *Group attributes* are composites or groupings of other attributes. For example, a group attribute ‘address’ may be a composite of ‘street’, ‘city’, ‘state’, and ‘zip code’. The third type, *semantic object attributes*, establish relationships between objects. In the PKI training database SOM, the ‘USER ROLE’ object contains the object attribute ‘TRAINING ELEMENT’. This indicates that there is a relationship between the ‘USER ROLE’ object and the ‘TRAINING ELEMENT’ object. The next step is to determine the nature of this relationship. That is done by determining the minimum and maximum cardinality.

Cardinality, in general, is the maximum or minimum number of elements allowed on each side of a binary relationship. *Minimum cardinality* indicates the number of instances of an attribute that must exist. This is normally 0 or 1. If the minimum cardinality is 0, then the attribute is not required to have a value. If the minimum cardinality is 1, the attribute must have a value for the relationship to be valid. *Maximum cardinality* is the maximum number of instances an attribute can have in a relationship. This value is typically 1 or N. If it is 1, the attribute can only have one instance. If it is N, the attribute may have several values with no specified limit. In the SOM, cardinalities are shown for each attribute in the format N.M. N is the minimum cardinality and M is the maximum cardinality. For example, in the ‘USER ROLE’ object the cardinality for the object attribute ‘TRAINING ELEMENT’ is 0.N. This means that each instance of ‘USER ROLE’ may have zero to many instances of ‘TRAINING ELEMENT’ associated with it. It is important to note that object attributes exist in pairs. The ‘TRAINING ELEMENT’ object attribute within the ‘USER ROLE’ class is coupled with the ‘USER ROLE’ object attribute within the ‘TRAINING ELEMENT’ class.

A complete SOM provides a great deal of information about how a database should be built. Together with the schema, the SOM can assist the developer in more

easily creating tables and relationships correctly. Once the database is built, summary information about it can be obtained. This information is called *metadata*.

4. METADATA

Metadata is defined as "data concerning the structure of data in a database stored in the data dictionary. Metadata are used to describe tables, columns, constraints, indexes, and so forth" (Kroenke, 2000, p. 577). Two tables of metadata were provided in Chapter V for the PKI training database. The first is table metadata. This lists each table, the number of columns (or fields) it contains, and the primary key for the table. The second is field metadata. This provides detailed information about the fields in each table. This information includes the data type, length, and description of each field.

With a schema, SOM, and metadata in hand, a great deal of information regarding a database is known. Attempting to build a database prior to developing these models and determining the descriptions of the data items would be difficult, time consuming, and potentially fall short of the requirements it is being built to fulfill. Although the models and techniques introduced in this appendix are only a few of the tools available, they can provide a solid foundation on which to build a database.

APPENDIX B. PROTOTYPE SCREENSHOTS

The following figures are screenshots of the prototype that was developed as a proof-of-concept for the proposed DoD PKI Training Framework.

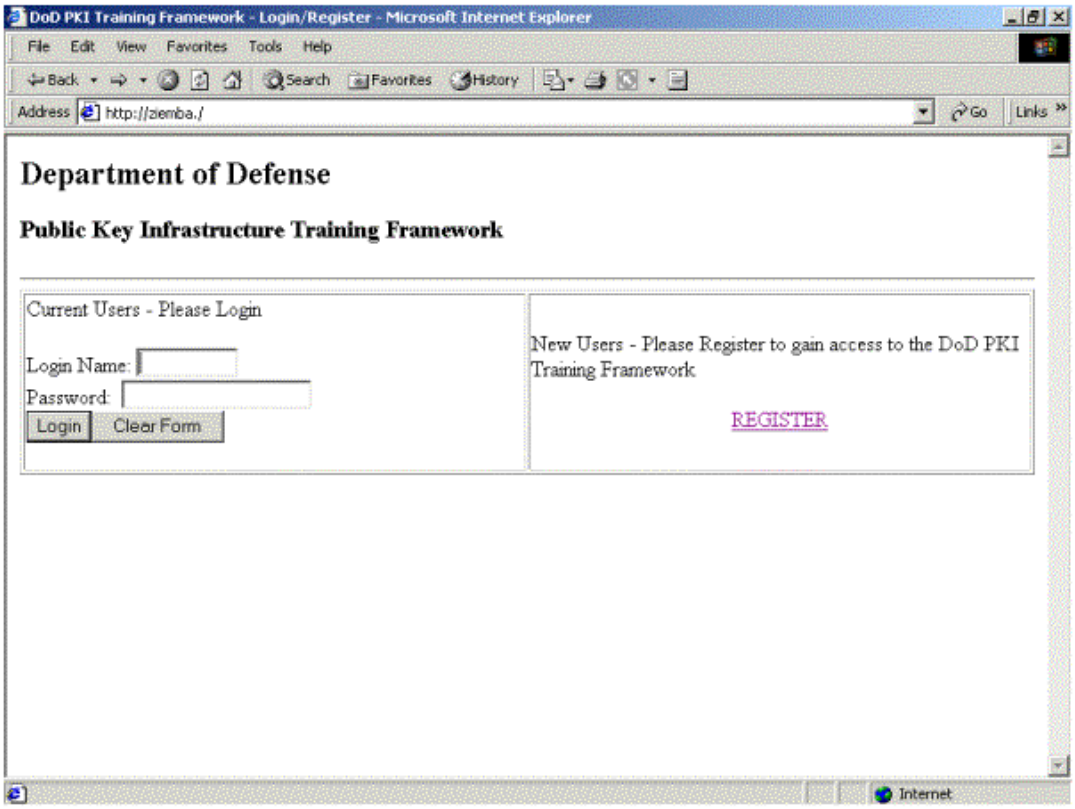

Figure B.1 Login Screen

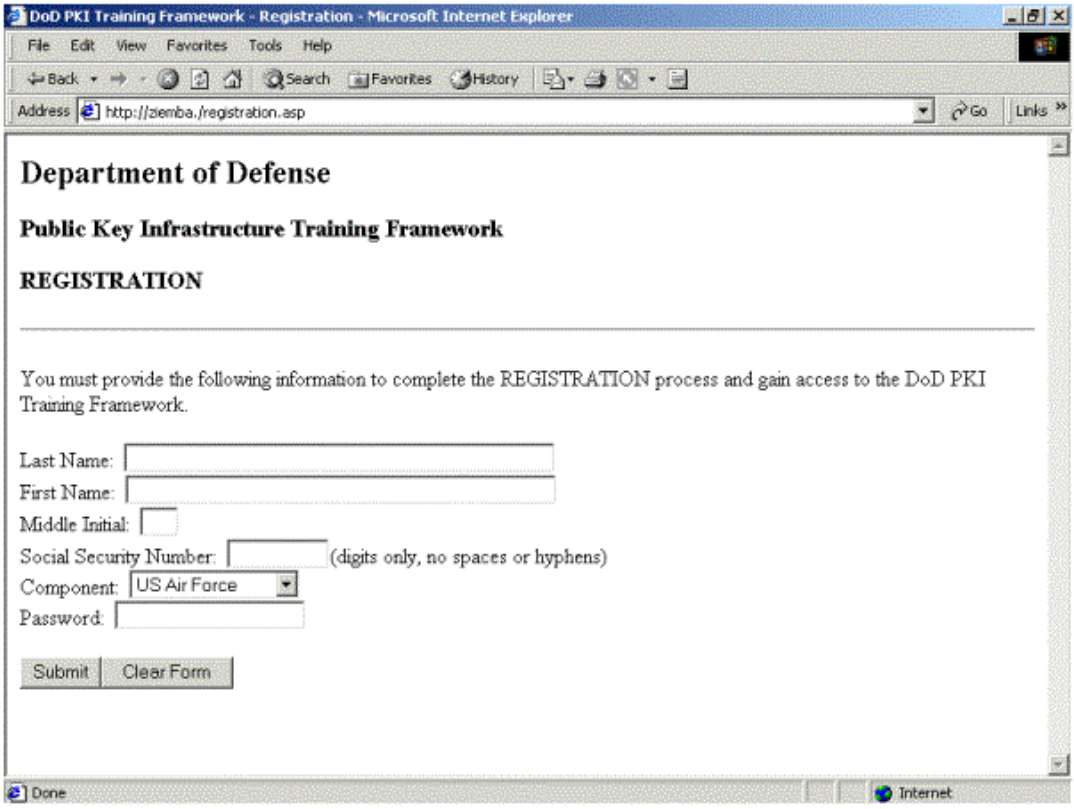

Figure B.2 Registration Page

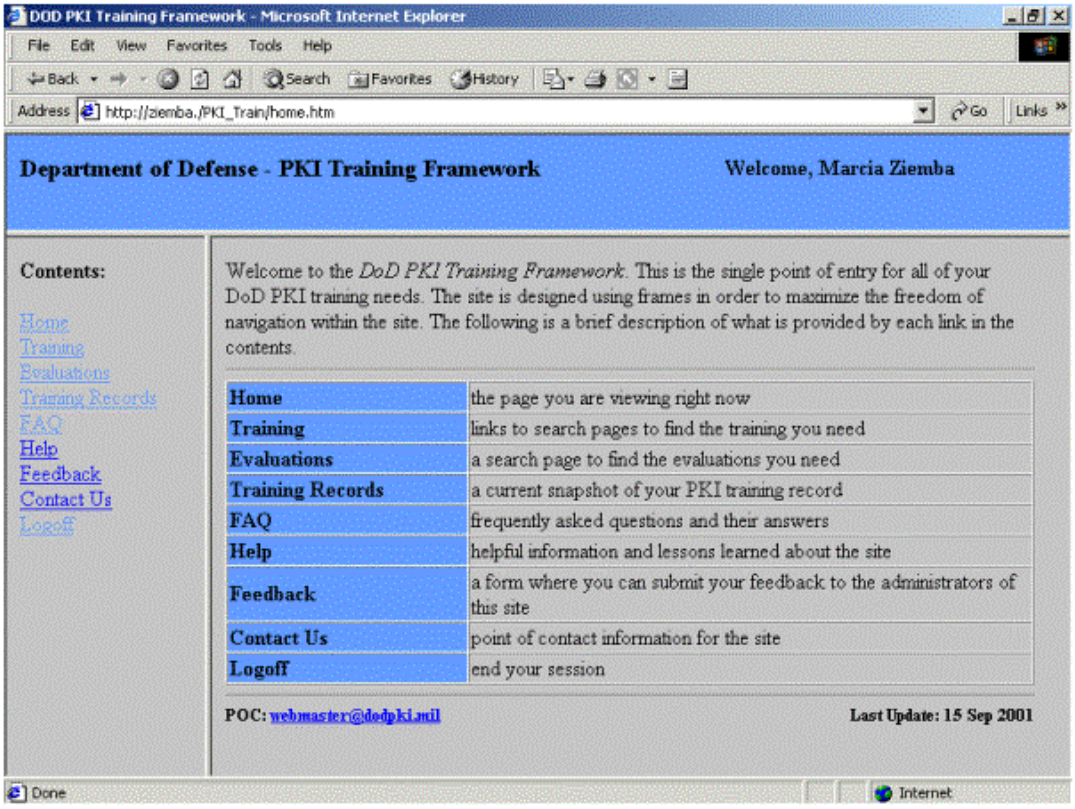

Figure B.3 Home Page

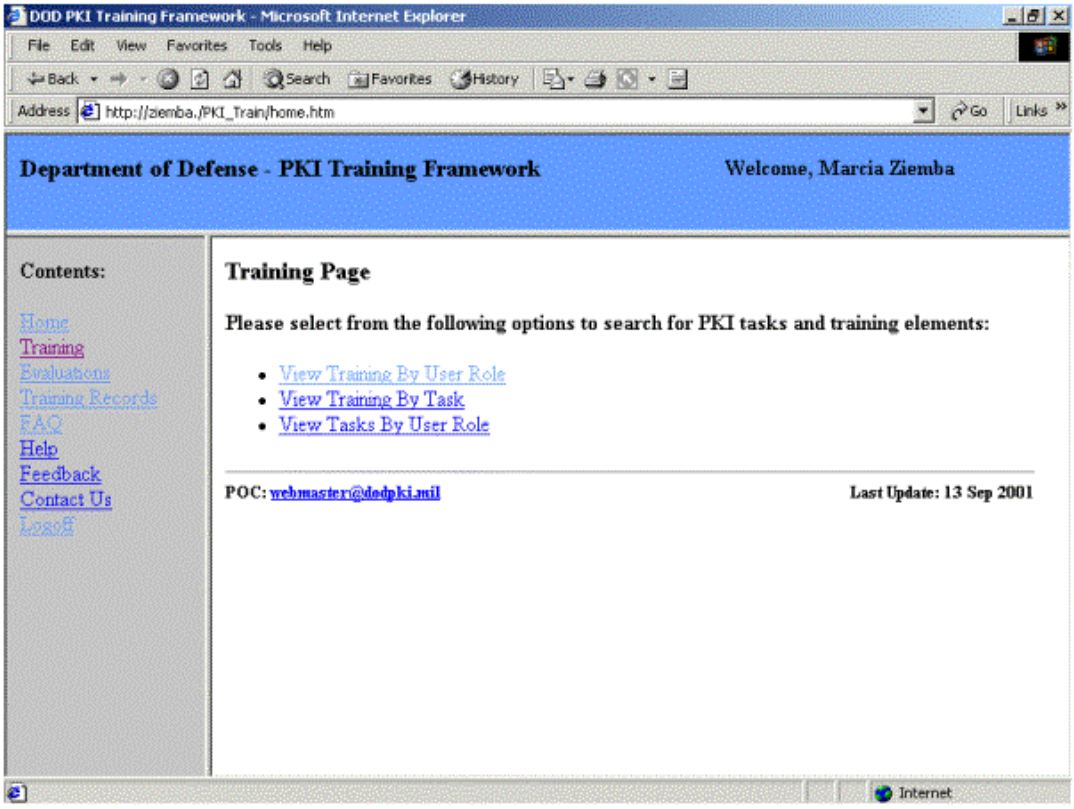

Figure B.4 Training Options Page

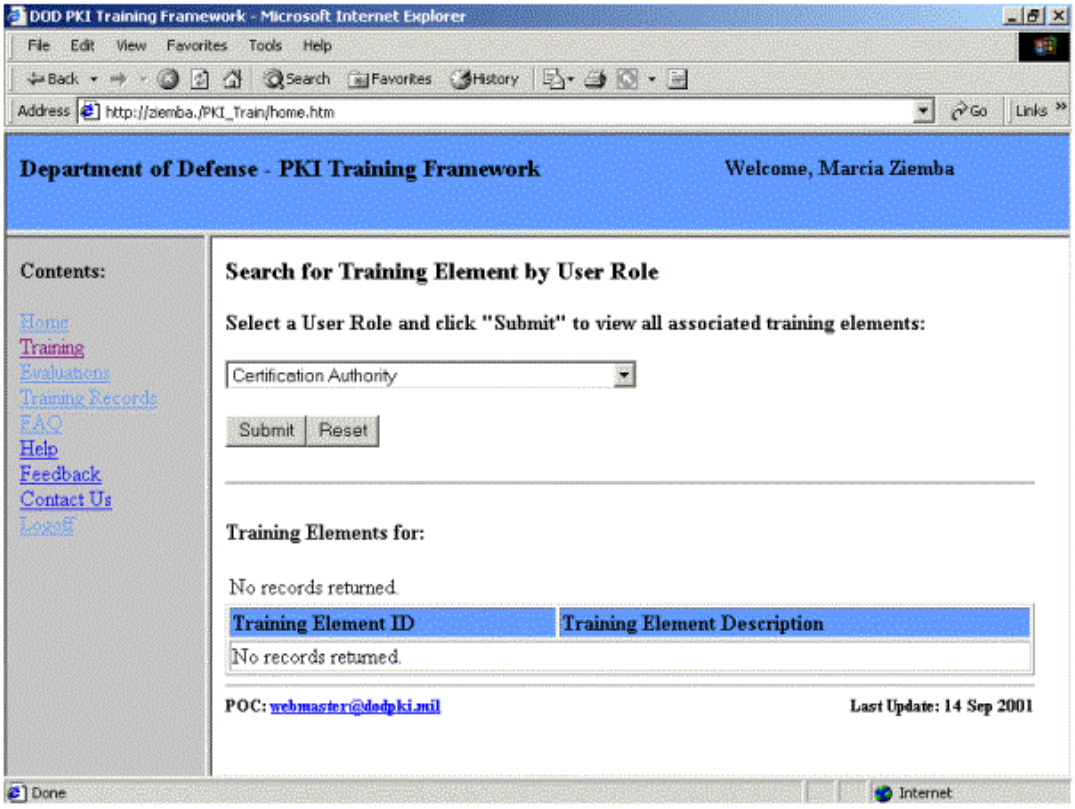

Figure B.5 Training By User Role Search Page

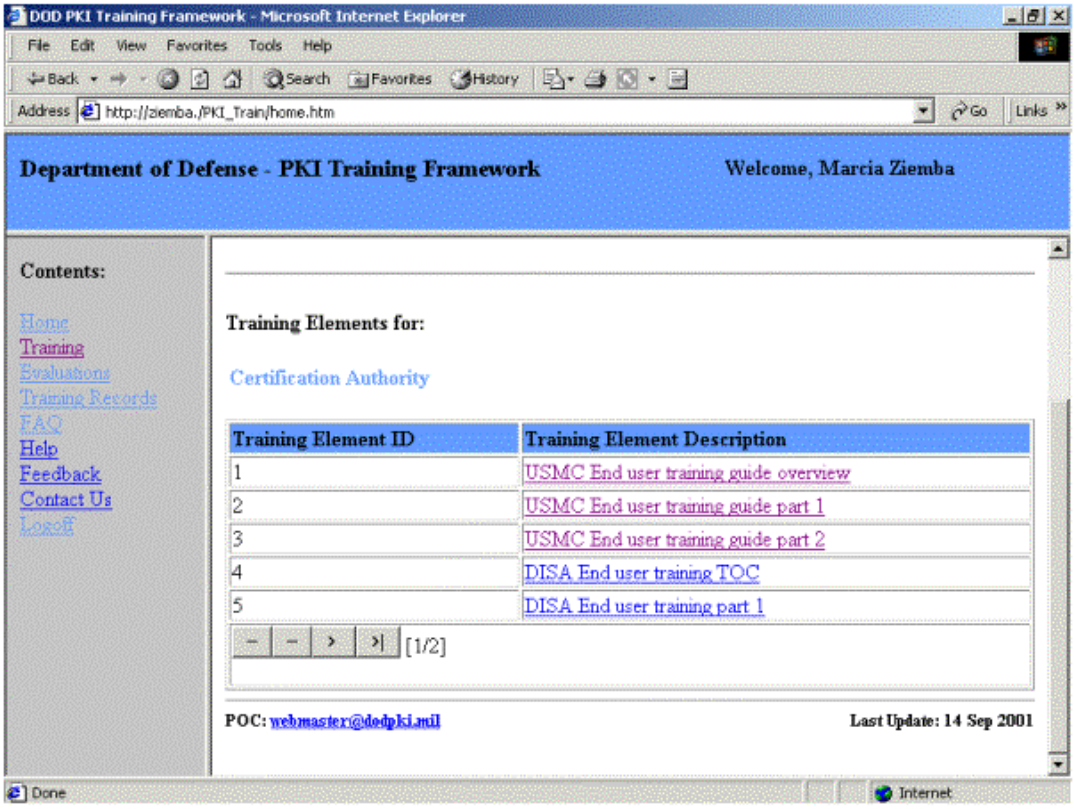

Figure B.6 Training By User Role Results

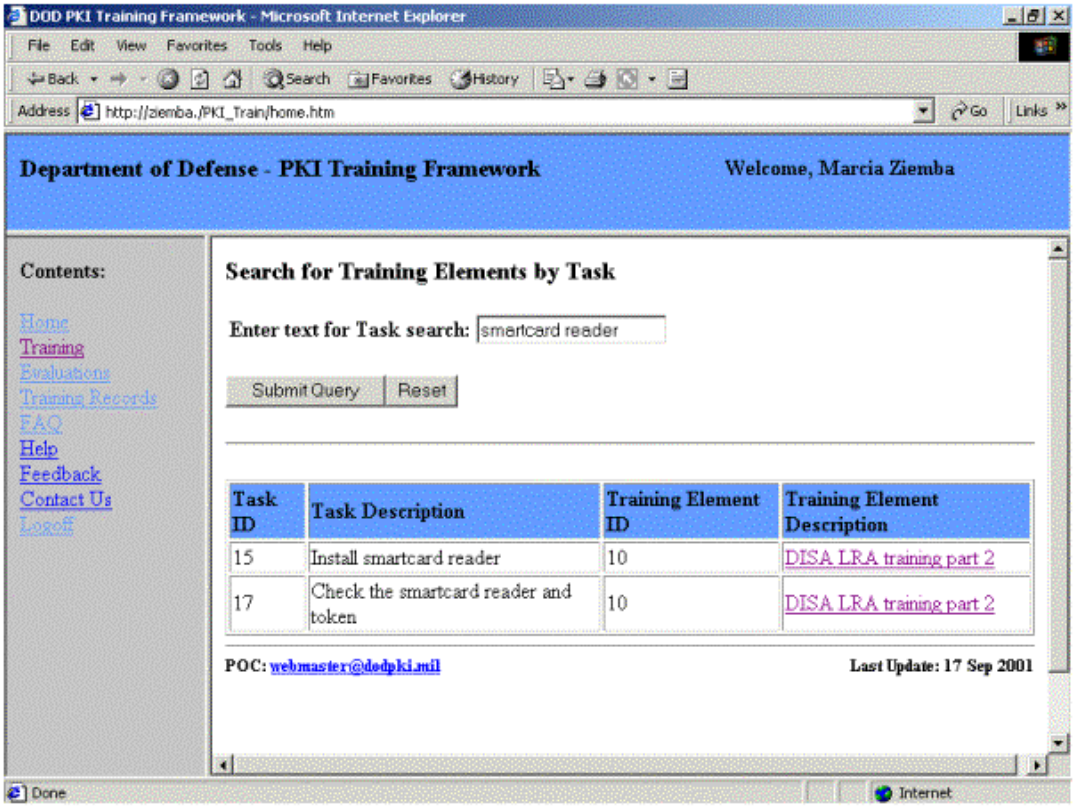

Figure B.7 Training By Task Page with Results

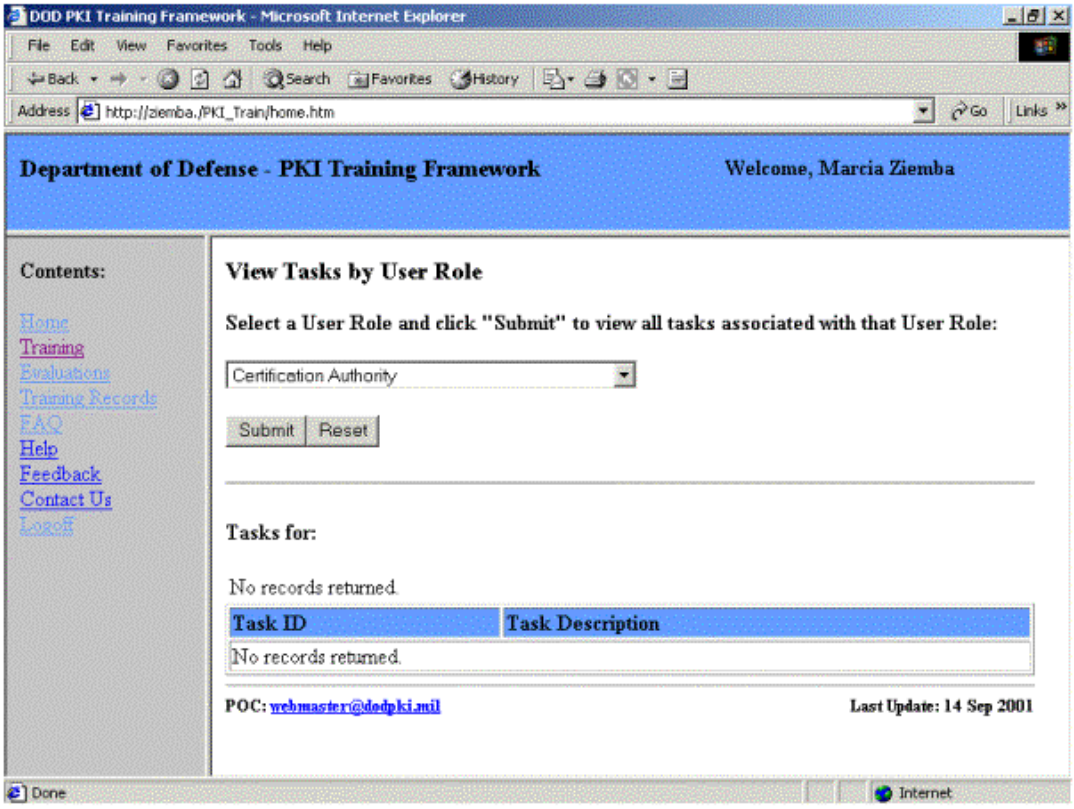

Figure B.8 Tasks By User Role Page

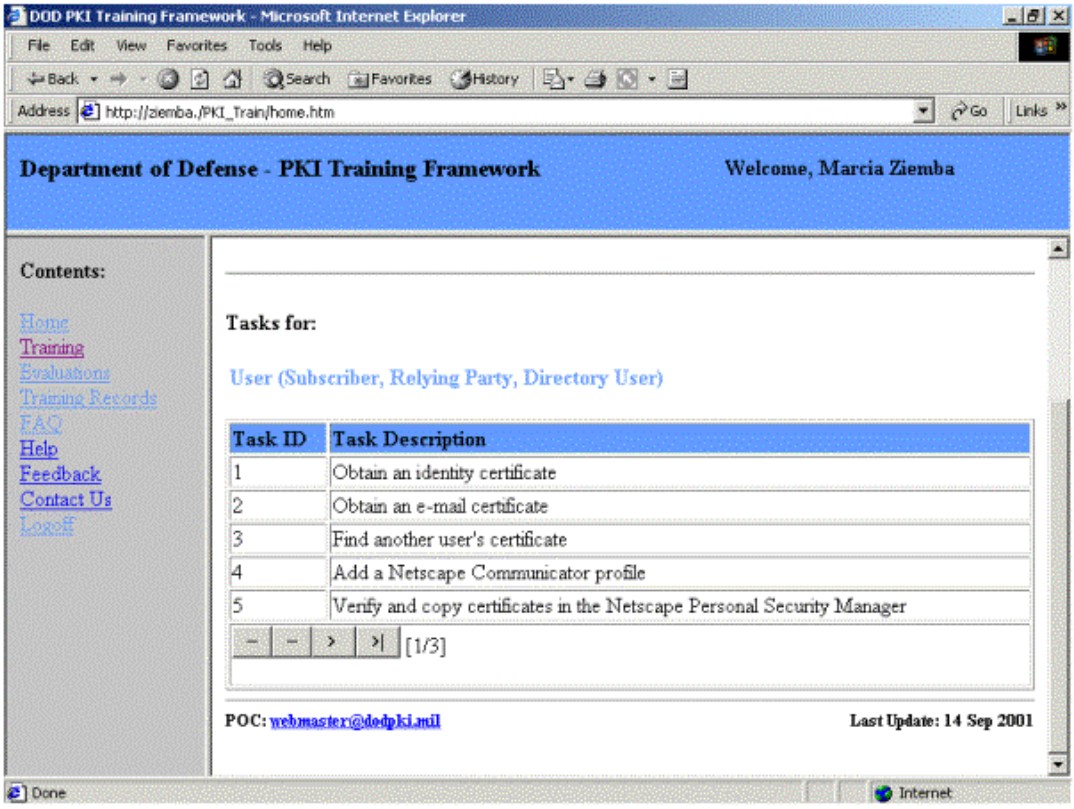

Figure B.9 Tasks By User Role Results

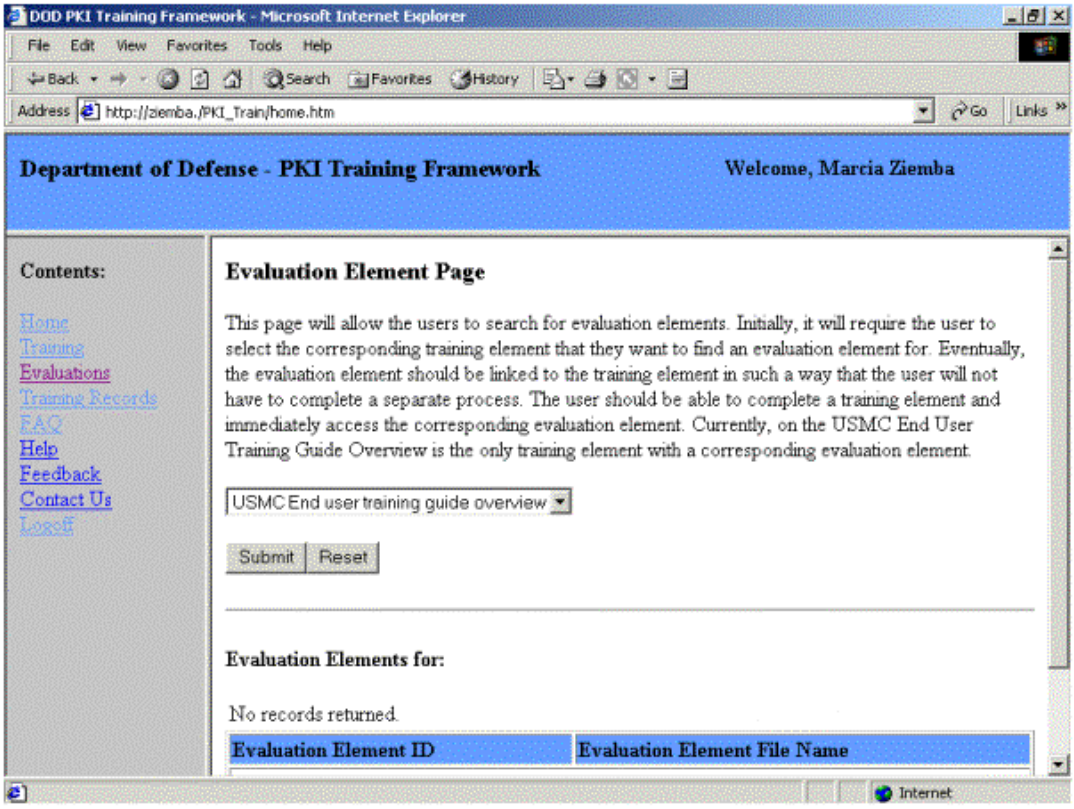

Figure B.10 Evaluation Element Page

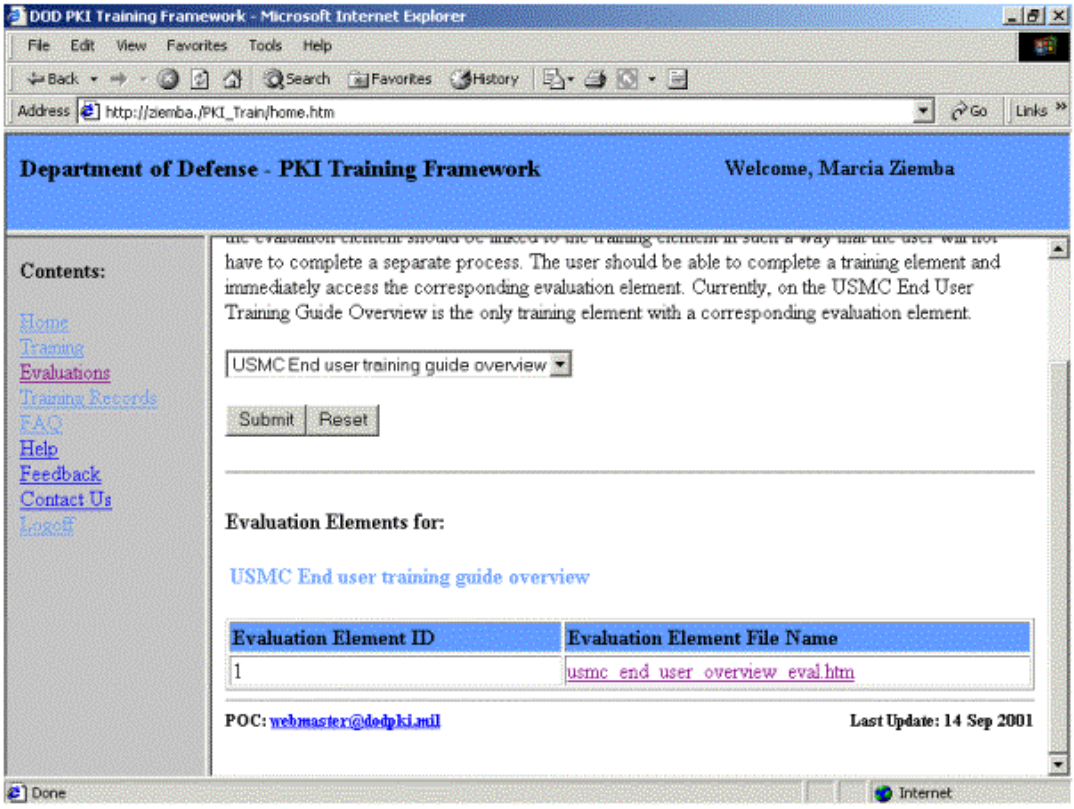

Figure B.11 Evaluation Elements Results

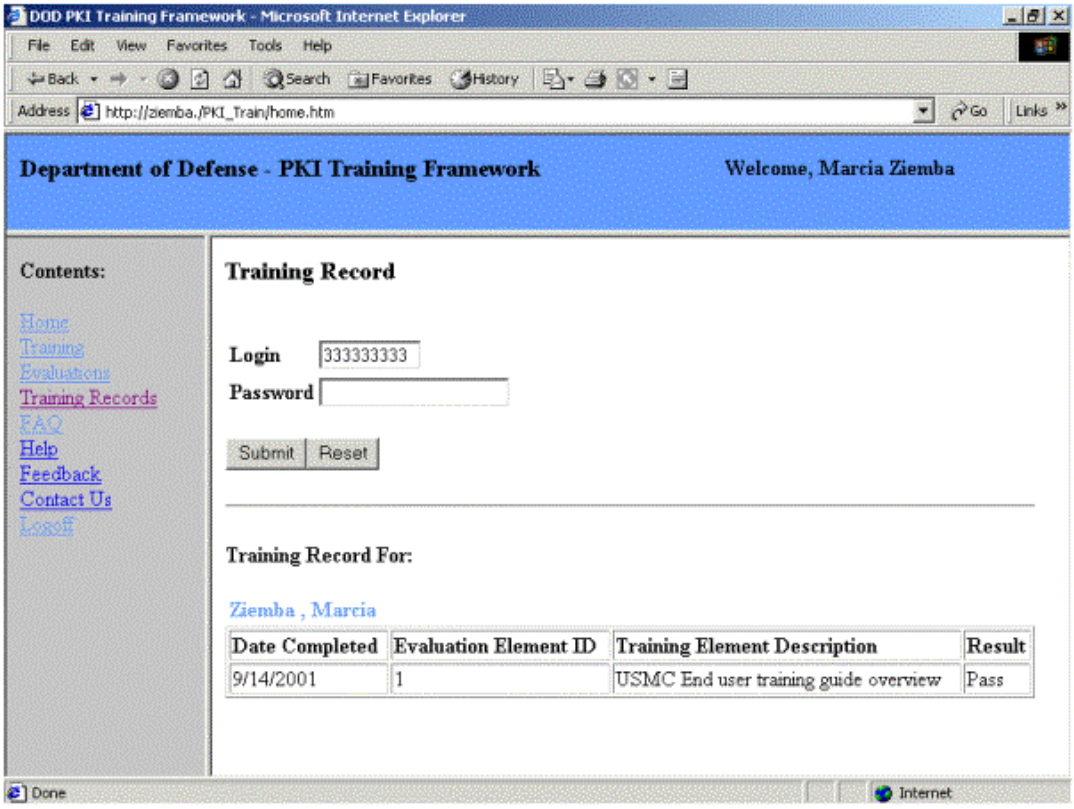

Figure B.12 Training Record Page

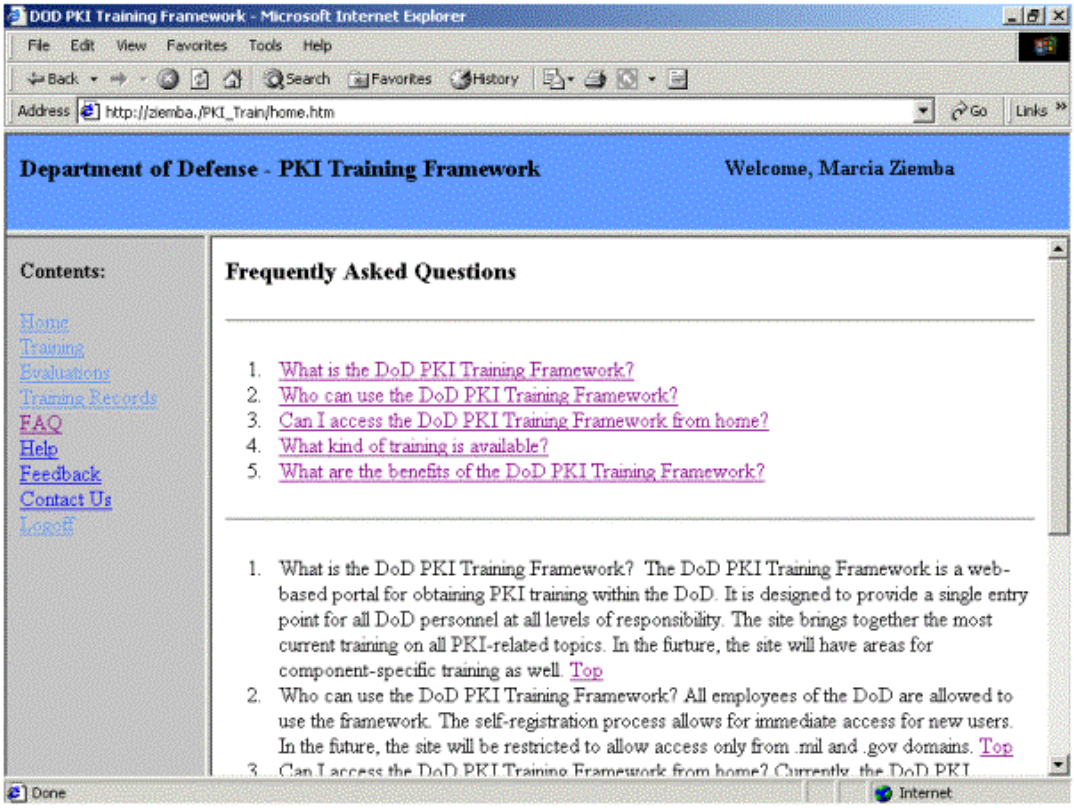

Figure B.13 Frequently Asked Questions Page

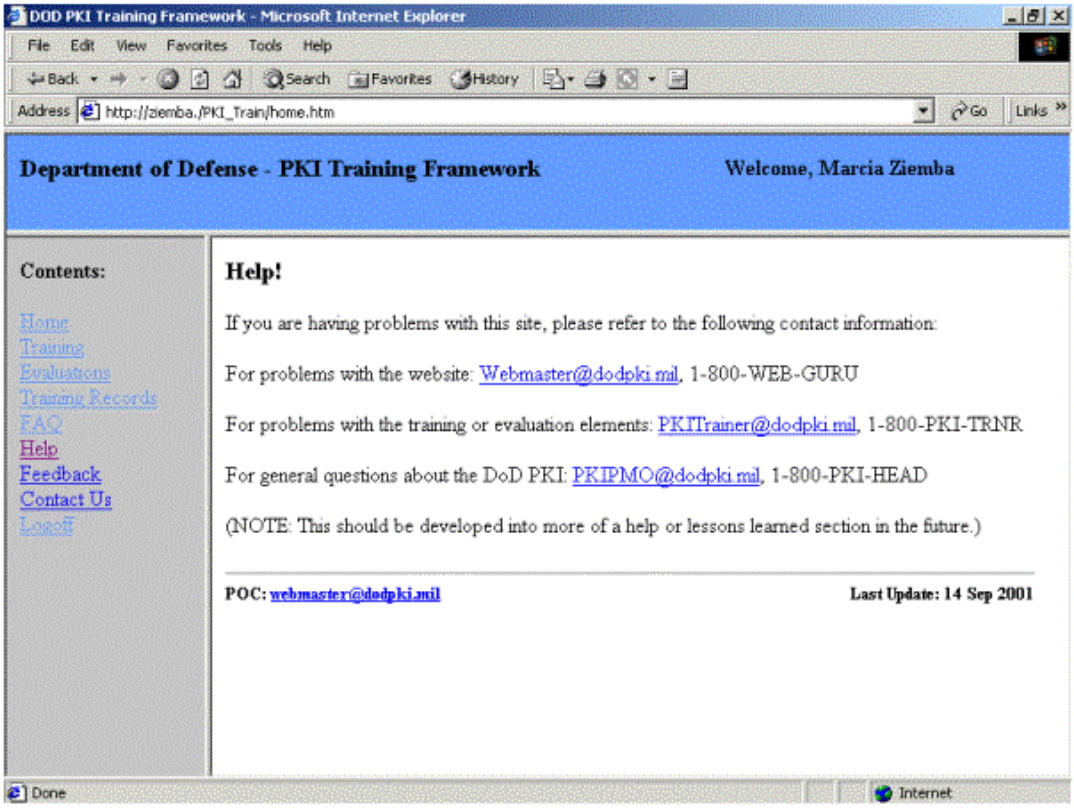

Figure B.14 Help Page

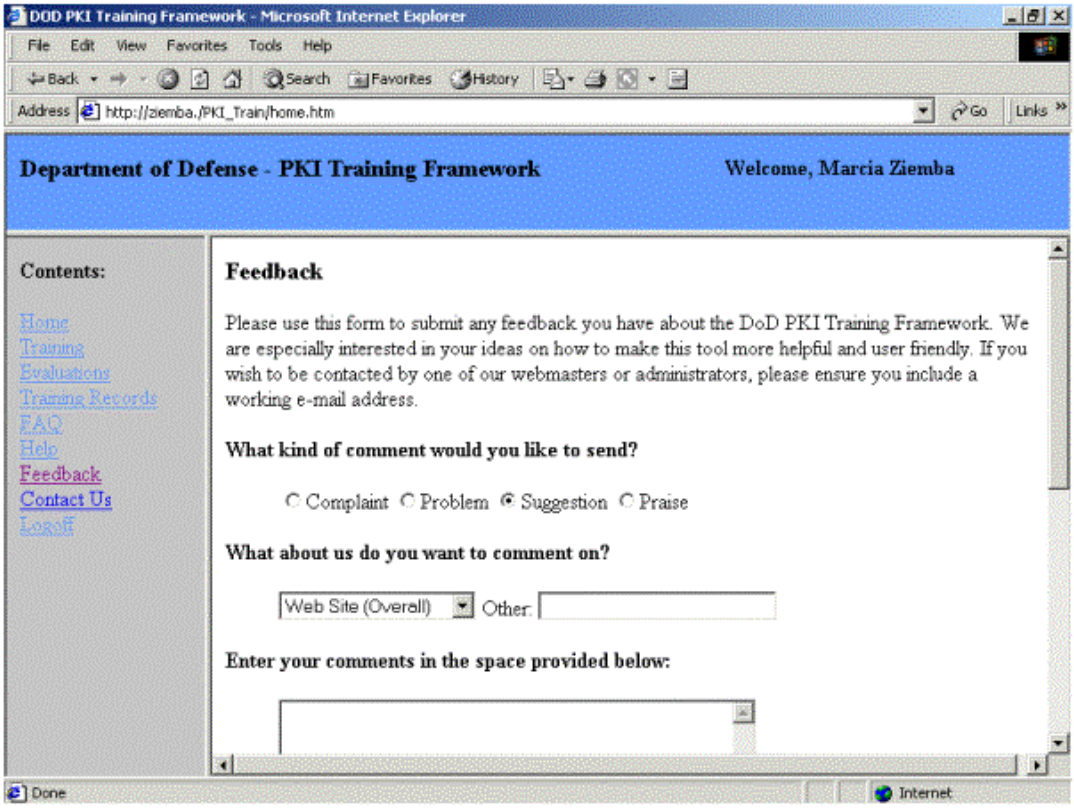

Figure B.15 Feedback Page

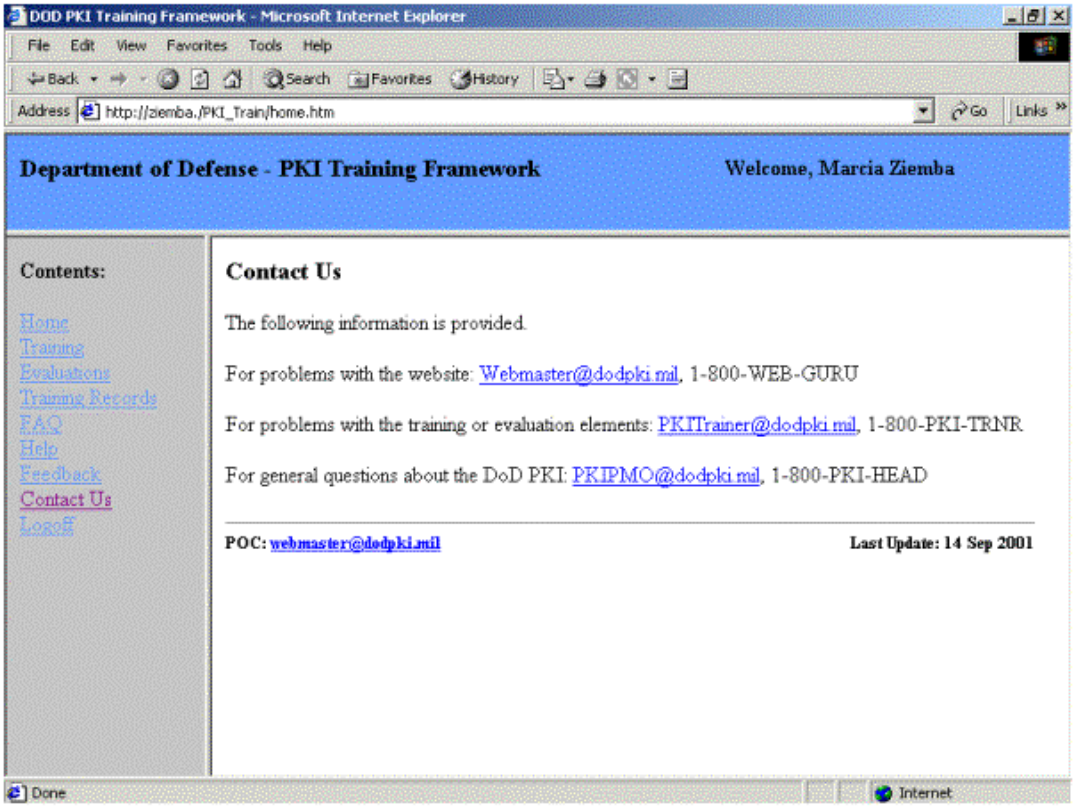

Figure B.16 Contact Page

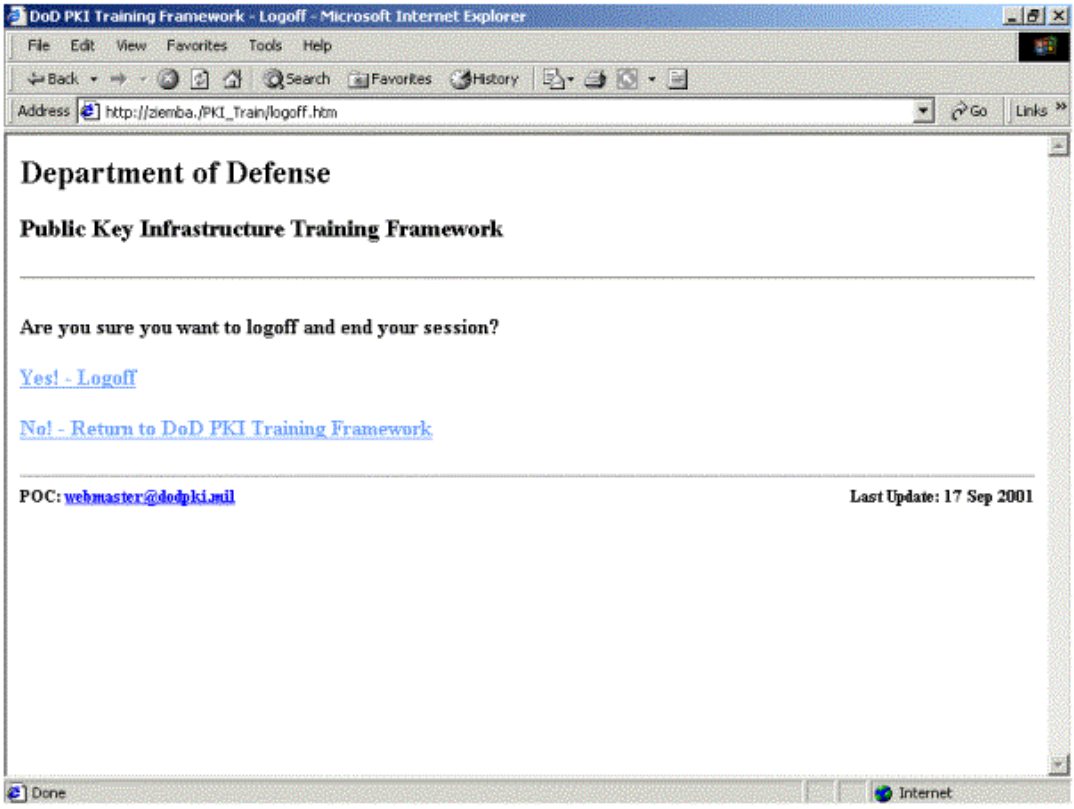

Figure B.17 Logoff Page

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

1. Adams, C. and Lloyd, S., *Understanding Public-Key Infrastructure – Concepts, Standards, and Deployment Considerations*, Macmillan Technical Publishing, Indianapolis, IN, 1999.
2. Alden, J., *A Trainer's Guide to Web-Based Instruction*, American Society for Training and Development, Alexandria, VA, 1998.
3. Assistant Secretary of Defense Memorandum, "Department of Defense (DoD) Public Key Infrastructure (PKI)," 12 August 2000, http://www.c3i.osd.mil/org/sio/ia/pki/.
4. Austin, T., *PKI: A Wiley Tech Brief*, John Wiley & Sons, Inc., New York, NY, 2001.
5. Berge. Z. L. (Ed.), *Sustaining Distance Training: Integrating Learning Technologies into the Fabric of the Enterprise*, Jossey-Bass, San Francisco, CA, 2001.
6. DISA, "Department of Defense Class 3 Public Key Infrastructure (PKI) End User Trainee Guide," July 2000, http://iase.disa.mil.
7. DISA, "Department of Defense Class 3 Public Key Infrastructure (PKI) Local Registration Authority (LRA) Trainee Guide," July 2000, http://iase.disa.mil.
8. DISA, "Department of Defense Class 3 Public Key Infrastructure (PKI) Registration Authority (RA) Trainee Guide," July 2000, http://iase.disa.mil.
9. DoD Public Key Infrastructure Program Management Office, "Public Key Infrastructure Roadmap for the Department of Defense, Version 3.0," 29 October 1999, http://www.c3i.osd.mil/org/sio/ia/pki/documents.html.
10. Gaines, L., *Trust and its Ramifications for the DOD Public Key Infrastructure (PKI),* Master's Thesis, Naval Postgraduate School, Monterey California, September 2000.
11. Galik, D., "PKI and the Navy", CHIPS, January 2000, http://www.norfolk.navy.mil/chips/archives/00_jan/pki.htm.
12. Gery, G., *Making CBT Happen: Prescriptions for Successful Implementation of Computer-Based Training in Your Organization*, Weingarten Publications, Boston, MA, 1987.
13. Green, R. M., "Public Key Infrastructure: The Enabler for DoD e-Bus," January 2001, rmgree2@missi.ncsc.mil.
14. Hale, R., "Introduction to Public Key Infrastructure and Applications," 7 May 1999, http://falcon3.ncr.disa.mil/Pki.pdf.
15. Hale, R., and Friedrichs, P., "Public Key Infrastructure (PKI) and the Use of Cryptography for Automating and Securing DoD Business Processes," http://www.knowledgenet.mil/knet/Feb00/Feb00.pdf, 28 January 2000.
16. Hall, B., *Training Management Systems: How to Choose a Program Your Company Can Live With*, Brandon Hall, Sunnyvale, CA, 1998.

17. “Introduction to Public-Key Infrastructure,” http://www.iplanet.com/developer/docs/articles/security/pki.html.

18. Kroenke, D. M., *Database Processing – Fundamentals, Design & Implementation (7th Ed.)*, Prentice Hall, Upper Saddle River, NJ, 2000.

19. Lynch, P. J., and Horton, S., *Web Style Guide: Basic Design Principles for Creating Web Sites*, Yale University Press, New Haven, CT, 1999.

20. Menezes, A., van Oorschot, P., and Vanstone, S., *Handbook of Applied Cryptography*, CRC Press, Boca Raton, FL, 1996.

21. Morris, D., “Public Key Infrastructure (PKI) Overview,” 2001, morrisde@hqmc.usmc.mil.

22. Morris, D., private communication, 16 May 2001.

23. Othman, S. F., e-mail message, 21 May 2001.

24. “Public Key Infrastructure – PKI,” http://www.id2tech.com/topmenu/smartcard/pki.asp.

25. Space and Naval Warfare Systems Command, “Medium Grade Service Messaging Primer, Version 1.0,” 3 April 2000, http://falcon3.ncr.disa.mil/index.html.

26. Steed, C., *Web-based Training*, Gower Publishing Limited, Brookfield, VT, 1999.

27. United States Marine Corps, “Public Key Infrastructure (PKI) End Users Class – Trainee Guide,” 2000, https://www.noc.usmc.mil/secure/PKI/default.htm.

28. United States Marine Corps, “Public Key Infrastructure (PKI) Local Registration Authority Class – Trainee Guide,” 2000, https://www.noc.usmc.mil/secure/PKI/default.htm.

29. “X.509 Certificates and Certificate Revocation Lists (CRLs),” http://java.sun.com/products/jdk/1.2/docs/guide/security/cert3.html.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, VA 22060-6218

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, CA 93943-5101

3. Carl Siel
   Space and Naval Warfare Systems Command
   PMW 161
   Building OT-1, Room 1024
   4301 Pacific Highway
   San Diego, CA 92110-3127
   sielc@spawar.navy.mil

4. Commander, Naval Security Group Command
   Naval Security Group Headquarters
   9800 Savage Road
   Suite 6585
   Fort Meade, MD 20755-6585

5. Ms. Deborah M. Cooper
   Deborah M. Cooper Company
   P.O. Box 17753
   Arlington, VA 22216
   d.cooper@computer.org

6. Ms. Louise Davidson
   N643
   Presidential Tower 1
   2511 South Jefferson Davis Highway
   Arlington, VA 22202
   davidson.louise@hq.navy.mil

7. Mr. William Dawson
   Community CIO Office
   Washington DC 20505
   williamf@odci.gov

8. Ms. Deborah Phillips
Community Management Staff
Community CIO Office
Washington DC 20505
deborlp@odci.gov

9. Capt. James Newman
N64
Presidential Tower 1
2511 South Jefferson Davis Highway
Arlington, VA 22202
Newman.James@HQ.NAVY.MIL

10. Major Dan Morris
HQMC
C4IA Branch
Navy Annex
Washington, DC 20380
MorrisDE@hqmc.usmc.mil

11. Mr. Richard Hale
Defense Information Systems Agency, Suite 400
5600 Columbia Pike
Falls Church, VA 22041-3230
haler@ncr.disa.mil

12. Ms. Barbara Flemming
Defense Information Systems Agency, Suite 400
5600 Columbia Pike
Falls Church, VA 22041-3230
flemingb@ncr.disa.mil

13. Mr. Michael Green, Director
Public Key Infrastructure Program Management Office
National Security Agency
9800 Savage Road
Ft. Meade, MD 20775
rmgree2@missi.ncsc.mil

14. Dr. Cynthia E. Irvine
Computer Science Department
Code CS/IC
Naval Postgraduate School
Monterey, CA 93943
irvine@cs.nps.navy.mil

15. Mr. Daniel Warren
Computer Science Department
Code CS/WD
Naval Postgraduate School
Monterey, CA 93943
warren@cs.nps.navy.mil

16. Mr. Dan Boger
Naval Postgraduate School
Monterey, CA 93943
dboger@nps.navy.mil